Kauno technologijos universitetas

Matematikos ir gamtos mokslų fakultetas

Bitkoino transakcijų klasifikavimas ir analizė

Baigiamasis magistro studijų projektas

Neringa Pacevič

Projekto autorė

Doc. dr. Kęstutis Lukšys
Vadovas

Doc. dr. Raminta Vaitiekūnienė
Vadovė

Kaunas, 2023

Kauno technologijos universitetas

Matematikos ir gamtos mokslų fakultetas

Bitkoino transakcijų klasifikavimas ir analizė

Baigiamasis magistro studijų projektas

Didžiųjų verslo duomenų analitika (6213AX001)

Neringa Pacevič
Projekto autorė

Doc. dr. Kęstutis Lukšys
Vadovas

Doc. dr. Raminta Vaitiekūnienė
Vadovė

Doc. dr. Audrius Kabašinskas
Recenzentas

Doc. praktikas Arvydas Jadevičius
Recenzentas

Kaunas, 2023

Kauno technologijos universitetas

Matematikos ir gamtos mokslų fakultetas

Neringa Pacevič

Bitkoino transakcijų klasifikavimas ir analizė

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjusi;

4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Neringa Pacevič

Patvirtinta elektroniniu būdu

Neringa Pacevič. Bitkoino transakcijų klasifikavimas ir analizė. Magistro studijų baigiamasis projektas /doc. dr. Kęstutis Lukšys /dr. Raminta Vaitiekūnienė; Kauno technologijos universitetas, Matematikos ir gamtos mokslų fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Taikomoji matematika (Matematikos mokslai).

Reikšminiai žodžiai: bitkoinas, bitkoino blokų grandinė, bitkoino transakcijų klasterizavimas, sukčiavimo aptikimas, transakcijų vertinimas, ekonominės veiklos.

Kaunas, 2023. 77 p.

Santrauka

Susidomėjimas bitkoinu bei blokų grandinėmis vis didėja. Kai 2008 metais atsirado bitkoinas bei buvo publikuotas bitkoino koncepto dokumentas, nedaug žmonių tikėjo bitkoino ateitimi. Pirmieji bitkoino metai nebuvo tokie populiarūs, tačiau bėgant laikui bitkoino populiarumas didėjo. Šiomis dienomis bitkoinas susilaukia didelio dėmesio tiek iš žiniasklaidos atstovų, tiek iš mokslininkų. Žiniasklaida dažnai publikuoja straipsnius, žinomų įmonių ar asmenų pasisakymus apie bitkoiną. Tuo tarpu mokslininkai analizuoja bitkoino blokų grandinę. Ypatingas dėmesys yra skiriamas sukčiavimo atvejų aptikimui. Yra sudarytas ne vienas modelis bei atliktas ne vienas tyrimas, siekiant paaiškinti bitkoino transakcijas bei kokia ekonominė veikla slepiasi po jomis.

Sukčiavimo atvejų aptikimui naudojami matematiniai metodai. Dažniausiai naudojami mašininio mokymosi metodai. Šio darbo tikslas yra naudojant matematinius metodus analizuoti bitkoino transakcijas, klasifikuoti, atpažinti įtartinas transakcijas bei suskirstyti jas pagal ekonomines veiklas. Bitkoino transakcijos yra viešai prieinami duomenys, todėl galima gauti reikalingus duomenis analizei tiesiog internete. Gauti duomenys yra apdorojami bei sudaromi bitkoino transakcijų grafai. Galutiniam duomenų rinkiniui yra pritaikomas klasterizavimas bei skirtingi jo metodai – k-vidurkių metodas, aglomeracijos metodas bei tankiu grįstas klasterizavimas. Šie metodų rezultatai yra palyginami tarpusavyje bei išrenkamas tinkamiausias klasterizavimo metodas bitkoino transakcijų duomenų rinkiniui. Taip pat analizės metu sudaromas bei pritaikomas transakcijų vertinimo koeficientas, kurio dėka galima vertinti pavienių transakcijų grafus atskirai, nepriskiriant grafų prie klasterių.

Pritaikytas klasterizavimo metodas bei sukurtas transakcijų vertinimo koeficientas leidžia suskirstyti transakcijas į atitinkamas keturias grupes. Kiekviena iš grupių turi tam tikrų bendrų požymių. Naudojantis rezultatais tyrime galima paaiškinti, kokios klasterių grupės atspindi kokias ekonomines veiklas. Rezultate taip pat išskirtas klasteris, kuris turi didžiausią kiekį įtartinų transakcijų. Klasterizavimo metodo bei transakcijų vertinimo koeficiento paskaičiavimais galima daryti išvadas apie transakcijos grafo skaidrumą. Šio tyrimo eigoje paaiškėjo, kad transakcijų vertinimo koeficientas gali padėti suskirstyti transakcijų grafus į atitinkamus klasterius. Tokiu būdu galima daryti išvadą, kad transakcijų vertinimo koeficientas gali būti naudojamas atskiram transakcijų grafui vertinti bei transakcijų grafai gali padėti identifikuoti skirtingas ekonomines veiklų rūšis.

Neringa Pacevič. Classification and analysis of bitcoin transactions. Master's Final Degree Project / supervisor /doc. dr. Kęstutis Lukšys vadovas /dr. Raminta Vaitiekūnienė; Faculty of Mathematics and Natural Sciences, Kaunas University of Technology. Study field and area (study field group): Applied Mathematics (Mathematical Sciences).

Keywords: bitcoin, bitcoin blockchain, transaction analysis, graph analysis, economic activities, fraud detection.

Kaunas, 2023. 77p.

Summary

Nowadays interest in bitcoin and the blockchain is very big. In 2008 when bitcoin was mentioned for the first time and bitcoin's white paper was published, not many believed in the future of bitcoin as currency. The first years of bitcoin were not so impressive, but step by step bitcoin became more and more popular. Nowadays bitcoin gets much attention from journalists, as well as from data scientists. While journalists are publishing articles, interviews with famous people related to bitcoin, data scientists are analyzing bitcoin blockchain. Special attention is dedicated to detecting money laundering cases in bitcoin blockchain. There are many mathematical models to analyze bitcoin blockchain, transactions and to explain what kind of economic activity is represented in those.

Money laundering cases are usually detected by mathematical models. There are usually used machine learning models which aim to classify, analyze transactions of bitcoin, identify suspicious transactions as well as divide it by possible economic activity. Data about bitcoin's transactions are publicly available on the internet. The data about bitcoin's transactions is used in this analysis. The transaction's data is used to create graphs. The final dataset includes properties about graphs as well as information about transactions. The final dataset is clustered using k-means method, agglomeration method and density-based clustering method. Results of these methods are compared together, and the best method is chosen. Also, during the analysis, there is created and used transaction evaluation coefficient, which helps to evaluate each transactional graph separately, without clustering data first.

After clustering analysis and evaluation of transactions using transaction evaluation coefficient, transactions were divided into four different groups. Each group represents common properties. Using the results of clustering, it is possible to explain which cluster is representing which economic activity. In the result, there is one cluster which has the most suspicious transactions of the block. It shows that clustering and transaction evaluation coefficient can help to predict which transaction is suspicious and should be investigated on a higher level. Also, during this analysis, it was noticed, that transaction evaluation coefficient can help to evaluate transactions separate, without processing clustering analysis first.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

Doc. – docentas;

Lekt. – lektorius;

Prof. – profesorius.

Terminai:

API – angl. *Application Programming Interface*. Interneto prieiga, leidžianti siųsti užklausas į interneto puslapio serverį bei gauti atsakymą.

Bitkoinas – pirmoji ir seniausia kriptovaliuta. Žymimas BTC simboliu.

Bloko maiša – bitkoino bloko grandinės identifikacinis tekstas sudarytas iš skaičių ir r aidžių.

Kriptovaliutų piniginė – virtuali tarlpykla, kurioje yra saugomos kriptovaliutos bei yra suteikiama galimybė jomis naudotis, tiek siųsti kitiems, tiek gauti.

Satošis – smulkiausioji bitkoino dalis, kuri yra lygi 0.00000001 bitkoino.

Transakcijos maiša – transakcijos identifikacinis tekstas sudarytas iš skaičių ir raidžių.

Transakcijos medis – bitkoino transakcijos bei transakcijos įvesčių grafas.

Įvadas

Bitkoinas atsirado 2008 metais. Iš pradžių susidomėjimas blokų grandine bei kriptovaliuta buvo nedidelis, ši naujovė atrodė daugumai nepatikima, tačiau po kelių metų susidomėjimas įgavo pagreitį. Bitkoinas yra dažnai minimas žiniasklaidoje, ekonomikos bei investicijų naujienose. Paskutiniais metais vis daugiau žmonių investuoja į bitkoiną. Vieni žmonės tiki kriptovaliutomis bei jų ateitimi, kiti laiko bitkoiną aukso atitikmeniu, treti žiūri skeptiškai. Bitkoino veikimo koncepte naudojama blokų grandinė yra sukurta taip, kad galėtų laisvai funkcionuoti pati, būti nepriklausoma nuo kitų finansinių institucijų ar kitų tarpininkų [3]. Bitkoinas susilaukia ir neigiamų komentarų. Pasaulyje, kuriame tvarumas yra viena iš pagrindinių temų, visas blokų grandinės veikimas, reikalaujantis didelių energijos resursų, nėra labai priimtinas [7]. Kita priežastis, dėl ko bitkoinas susilaukia kritikos, yra bitkoino kainos nepastovumas. Kainą gali paveikti daug išorinių veiksnių, o didžiausią įtaką daro finansinių institucijų ar įtakingų žmonių pareiškimai socialinėse erdvėse [55]. Nepaisant daugelio neigiamų komentarų, bitkoinas išlieka viena didžiausia, populiariausia kriptovaliuta. Bitkoino rinkos kapitalizacija yra viena didžiausių ir siekia net 518 milijardų JAV dolerių (2023 gegužės 13d.) [76]. Bitkoino blokų grandinė pasižymi savybėmis, kurios padeda išvengti finansinių institucijų tarpininkavimo sudarant sandorius [3]. Šios savybės pagreitina sandorių sudarymą, sandoriai yra atviri, visiems prieinami bei piniginių savininkai turi galimybę išlikti pseudo anonimiškais. Šios savybės, o ypač pseudo anonimiškumas, žavi sukčiautojus. Nuo bitkoino atsiradimo yra fiksuojamas ne vienas sukčiavimo atvejis, kurio metu bitkoinas buvo naudojamas nelegalioms veikloms remti.

Bitkoino naudojimas nusikalstamose veiklose kenkia bitkoino reputacijai, todėl reikia atrasti būdų, kaip tam užkirsti kelią. Šalių finansų institucijos tiria bitkoino blokų grandinę bei tikrina įtartinas pinigines, transakcijas, jų sumas, su kokiomis ekonominėmis veiklomis šios transakcijos yra susijusios. Ši sritis susilaukia daug dėmesio ne tik šalių vyriausybėse, tačiau ir tarp matematikų, duomenų mokslininkų. Mokslininkai bando pritaikyti įvairiausius matematinius metodus siekiant sukurti mechanizmą, kurio dėka pavyktų identifikuoti įtartinas veiklas bei tokiu būdu būtų galima užkirsti joms kelią. Mokslininkai dažniausiai susiduria su problema, kad duomenų kiekis yra labai didelis ir greitai didėja, todėl reikia gerų kompiuterinių resursų matematiniams metodams modeliuoti bei įvykdyti. Bitkoino blokų grandinė prijungia naują bloką prie grandinės vidutiniškai kas 10 minučių [77]. Viename bloke yra vidutiniškai 2 000 transakcijų [78]. Norint greitai pastebėti įtartinas veiklas, reikia apdoroti didelį kiekį duomenų bei tai atlikti ganėtinai greitai.

Šio darbo tikslas: naudojant matematinius metodus analizuoti bitkoino transakcijas, klasterizuoti, atpažinti įtartinas transakcijas bei suskirstyti jas pagal ekonomines veiklas.

Siekiant įgyvendinti šį tikslą, iškelti tokie **uždaviniai**:

1. Apžvelgti tyrimus susijusius su bitkoino transakcijų klasterizavimu bei bitkoino panaudojimu ekonomikoje, sukčiavimo atvejuose.
2. Sudaryti transakcijų grafus, kurie apimtų paskutinę transakciją bei prieš tai buvusias transakcijas.
3. Sudaryti duomenų rinkinį, kuris turėtų grafų informaciją bei papildomą transakcijų informaciją.
4. Pritaikyti matematinius metodus ir paskirstyti transakcijas į atitinkamas grupes. Sudaryti bei pritaikyti transakcijų vertinimo koeficientą, kuris padėtų įvertinti transakcijos parametrus.
5. Identifikuoti įtartinas transakcijas bei priskirti grupes atitinkamoms ekonominėms veikloms.

Mokslinėje tyrimo dalyje aptariama blokų grandinė ir jos sandarai, bitkoino savybės bei ypatumai. Nagrinėjama literatūra bei atlikti moksliniai tyrimai, kurie bando identifikuoti sukčiavimo atvejus naudojantis bitkoinu. Aptartos ekonominės veiklos bei bitkoino pritaikymas tose veiklose.

Darbo struktūra yra sudaryta iš trijų dalių. Pirma dalis apžvelgia literatūrą bei jau atliktus tyrimus. Antroje dalyje aptariami metodai naudojami tyrime. Trečioje dalyje aptariamas tyrimas bei jo eiga ir rezultatai.

1. Bitkoino transakcijų apžvalga

1.1. Bitkoino atsiradimo apžvalga

Bitkoinas yra pirmoji kriptovaliuta, kuri atsirado 2008 metais. Satoshi Nakamoto parašė dokumentą, kuriame apibūdino bitkoino konceptą [3]. Satoshi Nakamoto yra pseudonimas, kuriuo buvo pasirašytas bitkoino koncepto dokumentas. Jo tapatybė nėra identifikuota iki šiol, vieni teigia, kad tai gali būti net gi ne vienas asmuo o asmenų grupė, yra spekuliacijų, kad Satoshi gali būti Europos finansinio sektoriaus kolektyvas ar jo dalis. Satoshi Nakamoto atsiradus bitkoinu aktyviai dalyvavo bitkoino forume, atsakinėjo į klausimus, užregistravo domeną *bitcoin.org* bei dalinosi technine informacija apie bitkoiną forumuose. Pasak Satoshi Nakamoto, ši kriptovaliuta leis vykdyti tarpusavio sandorius saugiai nedalyvaujant jokiai trečiajai šaliai – finansinei institucijai, vyriausybei ar kitai įmonei. Taip pat dokumente teigiama, kad kadangi yra reikalaujami dideli resursai transakcijų pakitimams įvykdyti, todėl tai apsaugos tiek pirkėjus, tiek pardavėjus nuo galimo sukčiavimo, nes transakcijas pakeisti nebus taip paprasta.

Dėl savo koncepto, bitkoinas buvo laikytas anonimine valiuta, kurios transakcijas susieti su siuntėju ar gavėju neįmanoma. Todėl daugeliu atveju bitkoinas buvo pradėtas naudoti nelegalioje veikloje. Viena garsiausių tokių veiklų yra Šilko kelias. Tai internetinė juodoji rinka, kurioje buvo parduodami nelegalūs ginklai, padirbti dokumentai ir narkotikai. Skaičiuojama, kad apie 15 milijonų JAV dolerių buvo pervesta bitkoino transakcijomis, susijusiomis su Šilko kelio veiklomis 2012 metais [9]. 2013 metais FTB atsekė Šilko kelio organizatorius ir uždarė šią veiklą. Po Šilko kelio organizatorių atskleidimo buvo nustota manyti, kad bitkoinas yra anoniminė valiuta ir atsekti piniginės turėtojo neįmanoma.

Bitkoinas laikytas anonimine valiuta todėl, kad bitkoinai yra saugomi kriptovaliutų piniginėse. Sukurti kriptovaliutų piniginę gali bet kas, tam tereikia užsiregistruoti viename iš piniginių tinklalapių bei sugeneruoti piniginių maišos kodus. Piniginės turi du raktus: viešąjį raktą bei privatųjį raktą. Norint įvykdyti transakciją yra naudojamas viešasis raktas, o norint pasiekti transakciją – naudojamas privatusis raktas. Įprastai bankai ir kitos finansinės institucijos vykdo politiką „pažink savo klientą“, tokiu būdu jie privalo turėti duomenis apie sąskaitos savininką, jo adresą, vardą, pavardę, asmens identifikacijos numerį. Kriptovaliutų piniginę galima sukurti be asmens identifikacijos, nenurodant asmeninių duomenų, todėl ilgą laiką buvo manyta, kad bitkoinai yra saugi valiuta vykdyti transakcijoms, kurias neįmanoma atsekti. Žinoma, vykdant transakcijas iš vienos piniginės į kitą, atsekti lėšų savininką nėra lengva. Piniginės savininką galima identifikuoti tuomet, kai pinigai yra pervedami į kriptovaliutų keityklas. Norint konvertuoti bitkoiną į įprastą piniginę valiutą, reikia pervesti lėšas į kriptovaliutų keityklą ir tuomet atlikti keitimo operaciją. Tuo tarpu keityklos privalo rinkti informaciją apie savo klientus, panašiai kaip įprastos finansinės institucijos, todėl tokias lėšas, kurios buvo pervestos į keityklą, į asmens piniginę keitykloje, jau galima identifikuoti.

Yra du būdai kaip galima gauti bitkoiną, vienas jų yra bitkoino pirkimas keityklose, o kitas bitkoino iškasimas. Pirmasis būdas yra ganėtinai aiškus, bitkoiną galima įsigyti valiutų keityklose ar bitkoino biržose ir tuomet bitkoinas yra pervedamas į virtualią piniginę, kuri gali būti tiek virtuali, tiek fizinė. Bitkoino kasimas yra šiek tiek sudėtingesnis ir daugiau resursų reikalaujantis procesas. Kadangi bitkoinas yra decentralizuota valiuta, vadinasi, nėra jokio tarpininko, kuris patvirtintų, kad sandoris įvyko. Bitkoino sandoriai yra tvirtinami bitkoino kasėjų, o kasėjais gali tapti bet kas. Tam

reikia turėti pakankamai greitą kompiuterinę įrangą bei tam tikrą programinę įrangą. Bitkoino bendruomenė yra suinteresuota tapti kasėjais, kadangi gauna už tai atlygį. Įdomu tai, kad bitkoino kaina nėra priklausoma nuo kasėjų patiriamų išlaidų. Marthinsenas Johnas teigia [6], kad yra atvirkščiai, kai bitkoino kaina didėja (mažėja), didėja (mažėja) ir kasėjų patiriamos išlaidos.

Bitkoinas yra ypatingas tuo, kad dėl jo keičiama įprasta centralizuota sandorių sudarymo sistema. Elektroniniai mokėjimo sandoriai yra sudaromi decentralizuotai, kuomet sandoryje dalyvauja tik dvi šalys ir nėra trečiosios šalies, kuri patvirtintų sandorį [3]. Vietoje trečiosios šalies naudojami kriptografiniai skaičiavimai, todėl dvi šalys gali sudaryti sandorius be tarpininkų. Transakcijos įvykdomos, kuomet bitkoino kasėjų bendruomenė patvirtina transakcijas ir sukuria vadinamąjį bitkoino bloką, kurį prijungia prie prieš tai buvusio bloko. Kasėjai, patvirtindami transakciją, patvirtina, kad ta pati bitkoino moneta nėra išleista du kartus ir jie sukuria chronologišką transakcijų įvykdymo įrodymą.

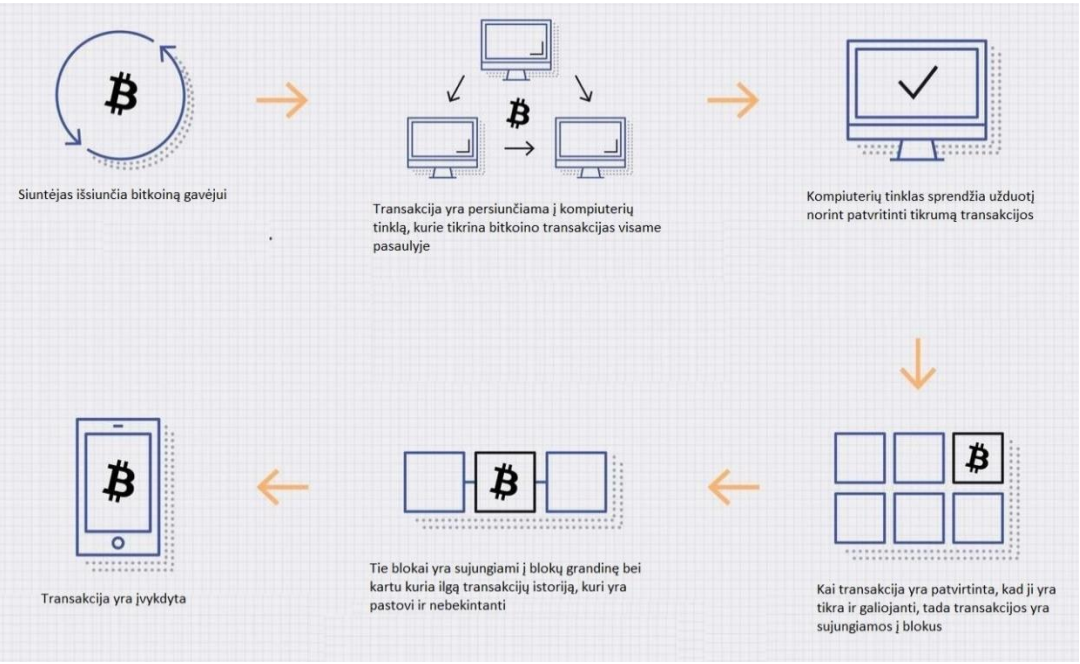
Bitkoino istorija prasidėjo 2008 metais spalio mėnesį, kuomet buvo parašytas dokumentas, aprašantis bitkoino konceptą. Tuo tarpu pirmoji transakcija įvyko 2009 metais sausio 3 dieną, kuomet Satoshi iškasė pirmąjį bitkoino bloką (angl. *genesis block*). Po kelių dienų Halas Finney buvo pirmasis, kuris parsisiuntė bitkoino programinę įrangą ir gavo 10 pirmųjų bitkoinų nuo Satoshi Nakamoto [8]. 2010 metais įvyko pirmasis sandoris bei 10 000 bitkoinų buvo iškeisti į dvi picas vietiniame Floridos restorane. Vėliau, 2010 metais rugpjūčio mėnesį, buvo pastebėtas vienintelis bei pats didžiausias iki šiol bitkoino saugumo iššūkis. Buvo pastebėta, kad vykdant transakciją, kurios išvesties suma yra didesnė nei 264 bitkoinai, transakcija įvyks ir tokiu būdu siuntėjas sukurs savavališkus bitkoinus. Jau po kelių dienų ši problema buvo pastebėta bei bitkoino blokų grandinė buvo atnaujinta naudojant atnaujintą bitkoino protokolą. Tokia problema daugiau nebepasikartojo. Kitos kriptovaliutos atsirado 2011 metais, kurios veikė panašiu principu kaip bitkoinas. Tais pačiais metais kelios organizacijos pradėjo priimti paramą bitkoinais. *Bitpay* yra pirmoji platforma, kuri priima mokėjimus bitkoinais. Platforma 2012 metais pranešė, kad yra sudariusi sutartis su daugiau nei 1 000 paslaugų tiekėjų, kurie priims mokėjimus bitkoino kriptovaliuta [33].

Bitkoinas tapo vis populiaresnis. 2013 metais keitykla *Coinbase* pranešė, kad per vasario mėnesį pardavė bitkoino monetų už 1 milijoną JAV dolerių, kurių kaina buvo apie 22 JAV dolerius [39]. Per kelis ateinančius mėnesius bitkoino kaina greitai keitėsi ir pakilo iš 22 JAV dolerių iki 266 JAV dolerių. Tuo metu jau vyko Šilko kelio nelegalūs veiksmai bei JAV vyriausybė birželio mėnesį pirmą kartą užšaldė 11,02 bitkoinų [35]. Vėliau, 2013 metais spalio mėnesį, FTB užšaldė 26 000 bitkoinų, kurie buvo susiję su Šilko keliu. Metų gale Kinijos centrinis bankas uždraudė Kinijos finansinėms institucijoms naudoti bitkoinus. Po tokio pranešimo bitkoino kaina smuko žemyn [34]. 2014 metais bitkoino kriptovaliuta buvo pradėta naudoti kai kuriuose video žaidimuose bei internetinių žaidimų platformose. Vis daugiau žinomų prekinių ženklų pradėjo priiminėti bitkoiną kaip mokėjimo valiutą. Netgi 2014 metų gruodžio mėnesį Microsoft leido atsiskaitymus bitkoinais, norint pirkti Xbox žaidimus ar Windows programinę įrangą [40]. 2015 metais įmonių ar organizacijų skaičius, kurios leidžia atsiskaityti bitkoinais, augo ir pasiekė 100 000 [36]. Vienos taikomojo meno muziejus buvo pirmasis, kuris pardavė meno kūrinį naudojant kriptovaliutas kaip mokėjimo valiutą [37]. Tais pačiais metais buvo pasiūlyta pridėti bitkoino valiutos ženklą prie universalių kodų sąrašo [38].

2016 metais Japonijos vyriausybė pripažino bitkoiną veikiant tokiu pačiu principu kaip įprastos piniginės valiutos [41]. Vis dar vyko bitkoino keityklų įsilaužimai. Rugpjūčio mėnesį *Bitfinex* keitykla prarado 120 000 bitkoinų, kurių vertė tuo metu siekė apie 60 milijonų JAV dolerių [42] bei tais metais daugėjo akademinių straipsnių bitkoino tema, atsirado pirmasis akademinis žurnalas *Ledger* [43]. 2017 metais įmonių skaičius, kurios priima atsiskaitymus bitkoinais, tik augo. Šalys, tokios kaip Japonija bei Rusija, pripažino kriptovaliutų mokėjimus kaip legalų mokėjimo tipą [44, 45]. 2018 metais Pietų Korėja įvedė reguliavimus, kurie reikalavo, kad bitkoinų prekiautojų asmenybės būtų identifikuotos [46]. Tokiu būdu siekiama sustabdyti kelią galimiems sukčiavimo atvejams, mokesčių slėpimo ar nelegalioms veiklos, ir sustabdyti kelią bitkoinų transakcijoms, kuriuose dalyvauja nepilnamečiai asmenys. 2019 metų gale bitkoino kaina siekė apie 4 000 JAV dolerių, o liepos mėnesį kaina buvo pakilusi net iki 12 000 JAV dolerių [47]. 2020 metais *Paypal* mokėjimų sistema leido vartotojams pirkti bei parduoti bitkoinus jų platformoje, tačiau bitkoinai negalėjo būti pervedami į arba iš kitos platformos ar piniginės į *Paypal* platformą [48]. 2021 metais bitkoinas pirmą kartą buvo leistas naudoti norint sumokėti mokesčius [49]. Taip pat didelio susidomėjimo sulaukė Elono Musko žingsnis, kuomet jo valdoma įmonė *Tesla* įsigijo bitkoinų, kurių vertė siekė 1,5 milijardus JAV dolerių, bei planavo priimti sprendimą leisti atsiskaitymus bitkoinais [51]. 2022 metais dėl karinės krizės Ukrainoje bitkoino kaina krito ganėtinai ženkliai. Balandžio mėnesį kaina nukrito iki 40 000 JAV dolerių, vėliau kaina krito dar labiau bei birželio mėnesį siekė mažiau nei 18 000 JAV dolerių. Ši kaina sugrįžo į 2017 metais pasiektą kainą [50].

1.2. Blokų grandinės sandara bei veikimo samprata

Bitkoinas yra sudarytas iš vadinamųjų blokų. Blokų grandinė saugo visus finansinius sandorius, sudarytus bitkoino tinkle [7]. Blokų grandinės samprata buvo pasiūlyta 2008 metais kartu su bitkoino kriptovaliutos konceptu. Ši idėja įgyvendinta 2009 metais, kai Satoshi Nakamoto iškasė pirmąjį bitkoino bloką. Bitkoino bloko iškasimas yra toks procesas, kurio metu patvirtinamos transakcijos.



1 pav. Bitkoino transakcijų tvirtinimo procesas [53]

Visų pirma, siuntėjas nori siųsti bitkoino sumą gavėjui. Tuomet yra suformuojama transakcija. Kompiuterių tinklas, kuris tikrina bitkoino transakcijų tikrumą, kad transakcijos būtų vienintelės, kad nebūtų ta pati bitkoino moneta išleidžiama kelis kartus. Kompiuterių tinklas vėliau sprendžia užduotį, kad patvirtinti transakciją. Tuomet patvirtintos transakcijos yra sujungiamos į bloką, tas blokas yra prijungiamas prie blokų grandinės bei naujame bloke yra buvusiojo bloko maiša. Kai naujas blokas yra iškastas bei prijungtas prie bitkoino bloko grandinės, tuomet transakcija yra patvirtinta bei gavėjas gauna lėšas.

Bitkoino blokai sudaro blokų grandinę, kurios blokai jungiasi tarpusavyje per kriptografijos blokų maišas. Tokiu būdu blokai sudaro grandinę, vadinasi, bloko transakcijos negali būti atšauktos ar pakeistos, tuo metu kai jos prijungiamos prie likusių blokų, nėra būdo pakeisti transakcijas. Blokas saugo informaciją pagrindinėje dalyje bei bloko antraštėje. Bitkoino bloko antraštė blokų grandinėje saugo informaciją apie [52]:

- Bitkoino bloko versija. Ši informacija parodo, kokių taisyklių reikia laikytis norint patikrinti transakcijų tikrumą.
- Buvusiojo bloko maiša. Maiša yra buvusiojo bloko identifikacija.
- *Merkle* medžio šaknies maiša. Maiša sudaryta iš visų *Merkle* medžio transakcijų bloke.
- Laikas. Laiko žyma (sekundėmis) kuomet bitkoino blokas buvo prijungtas prie blokų grandinės.
- *nBits*. Maišos objektas suspaustu formatu.
- *Nonce*. Koduotas skaičius, kurį bitkoino kasėjai turi surasti norint patvirtinti bloką bei prijungti jį prie blokų grandinės.

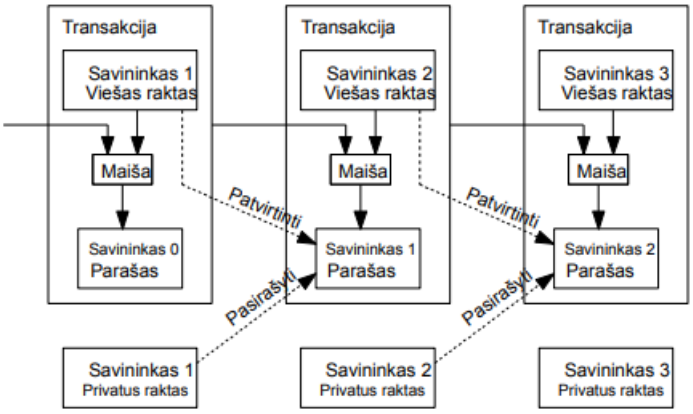
Tuo tarpu pagrindinė bitkoino bloko dalis saugo informaciją apie transakcijas. Kadangi blokai sudaro grandinę, kurios nebegalima pakeisti, tai yra saugus būdas vykdyti transakcijas. Bitkoino blokų grandinė užtikrina, kad kiekvienas veiksmas grandinėje yra įrašytas ir saugomas grandinėje, kuri turi visą informaciją ir laiko žymą. Tokiu būdų visi įvykę sandoriai yra prieinami viešai [10]. Bitkoino blokų grandinė taip pat yra decentralizuota, vadinasi, blokų grandinė nėra kontroliuojama finansinės institucijos ar visa informacija nėra saugoma tik viename kompiuteryje. Atvirkščiai – informacija yra paskirstyta po daugelį kompiuterių, kurie yra prisijungę prie bitkoino tinklo [10]. Vartotojai, dalyvaujantys bitkoino tinkle, atlieka tokius veiksmus [3]:

- perduoda naujas transakcijas visiems tinklo nariams;
- kiekvienas tinklo narys surenka ir sugrupuoja naujas transakcijas į naują bloką;
- kiekvienas tinklo narys prisideda prie bloko maišos radimo;
- kai tinklo narys galiausiai suranda tinkamą bloko maišą, jis perduoda informaciją kitiems tinklo nariams;
- likusieji tinklo nariai patikrina bloką ir transakcijas, esančias jame, jeigu jos yra galiojančios ir dar neišleistos, tuomet blokas yra patvirtinamas;
- tuomet tęsiamas darbas kitam blokui, pastarojo bloko maiša yra naudojama kitame bloke.

Anot Satoshi Nakamoto [3], vienintelis būdas pakeisti jau įvykdytas transakcijas yra pakeisti būtent to bloko maišą bei visų kitų blokų maišas. Tai turėtų būti padaryta greičiau nei sąžiningi bitkoino tinklo nariai prijungia naują bloką prie bitkoino grandinės. Galimybių tai padaryti beveik nėra, nes nauji blokai atsiranda ganėtinai greitai, juolab, kad kuo greičiau atsiranda blokai, tuo sunkiau yra atrasti tinkamą bloko maišą, nes algoritmas vis sunkėja.

1.3. Bitkoino transakcijų vykdymo apžvalga

Bitkoino koncepto dokumente [3] rašoma, kad transakcija yra nusakoma skaitmeninių parašų grandine. Yra du tipai bitkoino transakcijų: vieną jų vadiname pradine (angl. *coinbase*) transakcija, kitą – įprasta transakcija. Pirminė transakcija yra pirmoji transakcija naujai iškasto bitkoino bloke, tai yra apdovanojimas bitkoino tinklo nariams už darbą, prijungiant bloką prie blokų grandinės. Tokiu būdu naujos bitkoino monetos yra įtraukiamos į apyvartą. Įprastos transakcijos yra visos kitos transakcijos, kurių metu vykdomi sandoriai [9]. Bitkoino savininkas, norėdamas įvykdyti transakciją, persiunčia bitkoiną kitam savininkui, pasirašydamas buvusiosios transakcijos maišą su viešu gavėjo raktu, ir tuomet bitkoino transakcija pridedama prie transakcijų sąrašo galo.



2 pav. Bitkoino transakcijų siuntimo paaiškinimas [3]

Tokiu būdu galima atsekti visas buvusias transakcijas, kuriose dalyvauja būtent ta bitkoino moneta, bei pamatyti duomenis apie buvusias transakcijas ir savininkų piniginių. Transakcijos susideda iš tokios informacijos [54]:

- Įvesčių informacija. Kiekviena transakcija turi informaciją apie buvusiąją transakciją. Tarkime, Jonas siuntė Petrui 0,6 bitkoinus ir Juozas siuntė Petrui 0,6 bitkoinus. Tuomet Petro transakcijoje Alisai 1 bitkoino įvestys bus 0,6 transakcija iš Jono Petrui bei 0,6 transakcija iš Juozo Petrui. Tokiu būdu perduodama visa informacija apie buvusias transakcijas.
- Transakcijos suma. Šio pavyzdžio atveju transakcijos suma yra 1 bitkoinas.
- Išvesčių informacija. Šio pavyzdžio atveju bus dvi išvestys. Viena išvestis yra Alisai 1 bitkoinas, o kita yra 0,2 bitkoino grąža Petrui.

Matome, kad transakcijose yra informacija ne tik apie tai, kur keliauja lėšos, tačiau ir iš kur tos lėšos yra gautos.

Vienas iš iššūkių bitkoino tinklo nariams yra įsitikinti, kad siunčiamas bitkoinas nebuvo panaudotas du kartus. Kad to išvengti, atliekant kiekvieną transakciją, bitkoinas grįžta į bitkoinų kasyklą. Jeigu transakcija yra patvirtinama, tuomet iš kasyklos išduodamas naujas bitkoinas ir įvyksta sandoris bei naujas savininkas gauna pervedamą sumą. Kasykla vaidina svarbų vaidmenį šitame procese, kadangi jie yra atsakingi už pirmosios transakcijos patvirtinimą, kad išvengti dviejų galimų transakcijų naudojant tą patį bitkoiną. Taigi, kasykla turi žinoti apie visas iki šiol buvusias transakcijas, kad kasyklos tinklo nariai galėtų patvirtinti pirmutinę transakciją [3].

Bitkoino tinklo nariai tokiu būdu formuoja bitkoino grandinės bloką. Bloke yra apjungiamos transakcijos, kurios yra patvirtintos. Kai bitkoino tinklo narys suformuoja bitkoino grandinės kitą bloką, tuomet blokas yra siunčiamas bitkoino tinklo nariams patikrai [54]. Jeigu kiti bitkoino tinklo nariai sutinka, kad šis blokas yra teisingas bei visos transakcijos jame yra teisingos, tuomet blokas prijungiamas prie bitkoino bloko grandinės bei tie nariai, kurie pasiūlė šį bitkoino grandinės bloką, gauna apdovanojimą – tam tikrą bitkoino sumą, dar gi jie gaus visus transakcijų, esančių tame bloke, mokesčius. Kiekviename bloke yra ribotas skaičius transakcijų, todėl kad vienas blokas užima 1 MB vietos. Taigi, norint, kad siunčiama transakcija pasiektų gavėją kuo greičiau, reikia sumokėti didesnį transakcijos mokestį, nes bitkoino tinklo nariai labiau linkę rinktis didesnio mokesčio transakcijas bei jas patvirtinti naujame bloke. Tokiu būdu jie gauna didesnį apdovanojimą. Taigi, siuntėjas gali pats nuspręsti, ar nori mokėti didesnį transakcijos mokestį, kad transakcija būtų patvirtinta greičiau, ar sutinka laukti ilgiau ir transakcija bus patvirtinta tuomet, kai bitkoino tinklo nariai turės mažesnį kiekį nepatvirtintų transakcijų bei neturės tokio didelio transakcijų pasirinkimo [54].

1.4. Bitkoino kaip valiutos privalumai bei patrauklumas

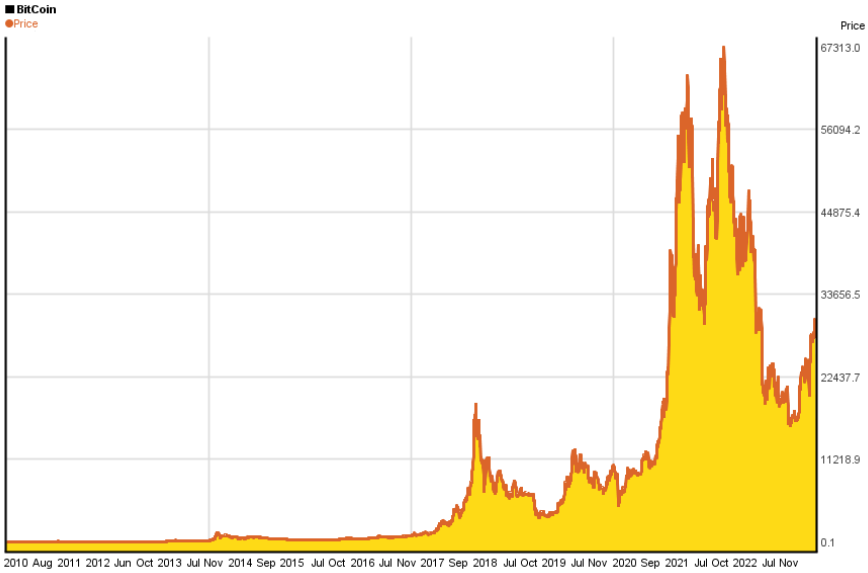
Blokų grandinė pasižymi savo privalumais, kurių nėra įprastoje valiutų sistemoje. Tai padeda bitkoino kriptovaliutai pelnyti populiarumą. Šios bitkoino savybės priklauso nuo blokų grandinės veikimo principo [12]:

1. Decentralizuota sistema. Bitkoino blokų grandinė nepriklauso nuo vieno kompiuterio ar vienos finansinės institucijos, įmonės.
2. Transakcijos yra nekintančios. Nėra galimybių arba jos ypatingai menkos, kad pakeisti buvusią transakciją.
3. Skaidrumas. Transakcijų duomenys yra prieinami kiekvienam bitkoino tinklo nariui, todėl bloko grandine galima pasitikėti.
4. Atvirumas. Transakcijos yra prieinamos viešai kiekvienam norinčiam sužinoti daugiau apie jas. Jas galima pasiekti internete be didelių sunkumų.
5. Anonimiškumas. Transakcijos gali išlikti anonimiškos, svarbu žinoti tik viešąjį gavėjo piniginės raktą. (Jeigu transakcijos bus pervedamos naudojantis bitkoino keityklomis, tokiu atveju yra galimybė atsekti lėšų savininkus, tačiau jei sandoris vykdomas be keityklų, anonimiškumas išlieka.)

Šios pagrindinės bitkoino blokų grandinės savybės daro šią kriptovaliutą patrauklią naudojimui.

1.5. Bitkoino kaip valiutos vertinimas

Pačioje pradžioje vyravo skirtingos nuomonės apie bitkoiną kaip valiutą. Vieni tikėjo šios valiutos ateitimi, kiti buvo skeptiški todėl, kad lygino bitkoino valiutą su įprasta pinigine valiuta. Davidas Hume teigia [4], kad piniginė valiuta yra padengta auksu arba sidabru bei norint prognozuoti piniginės valiutos kursą, aukso ar sidabro kaina yra ignoruojama. Vėliau buvo pastebėta, kad aukso ar sidabro vertės ignoravimas padeda prognozuoti kaip visa piniginės valiutos suma keisis su piniginės valiutos kiekiu. Jeigu lygintume įprastą piniginę valiutą su bitkoinu, tai bitkoinas nėra padengtas auksu ar sidabru ar kuo kitu, todėl ir jų kainos ignoruoti nereikia. Davidas Hume netgi teigia, kad blogiausiu atveju bitkoino negalima būtų panaudoti net kaip tapetų, kaip kad buvo naudojamos Vokietijos markės per 1922-1923 hiperinfliaciją.



3 pav. Bitkoino kainos grafikas [55]

Bitkoino vertė bitkoino atsiradimo pradžioje buvo stabili ir maža. Pati pirmoji bitkoino transakcija buvo atlikta atsiskaitant už dvi picas, kurių kaina siekė 10 000 bitkoinų [23]. Vėliau 2010 metais atsirado *MT Gox* keitykla, kurioje 20 bitkoinų buvo iškeisti už mažiau nei 1 JAV dolerį. Prireikė poros metų, kad bitkoino kaina pakiltų iki 100 JAV dolerių. 2012 metais bitkoino kaina pasiekė aukštumas, jo vertė siekė net 1 238 JAV dolerius. Vėliau kaina krito ir kitas pakilimas buvo po ketverių metų, 2016 metais, kuomet bitkoino kaina siekė net 20 000 JAV dolerių. Kitas didžiausias kainos pakilimas buvo, vėlgi, po ketverių metų, 2020 metais, ir kaina siekė net beveik 69 000 JAV dolerių. Matoma tendencija, kad kaina kelis metus kyla ir ketvirtais metais kaina sustoja, šiek tiek sumažėja ir tada krenta žemyn.

Didelę įtaką bitkoino kainos svyravimams turi socialinė erdvė. Ullahas savo tyrime [24] atskleidė, kad yra labai ženklus neigiamas poveikis bitkoino kainai, jeigu socialinėje erdvėje atsiranda neigiami komentarai ar kiti pareiškimai iš valstybinių institucijų. Vadinasi, komentarai iš valstybinių arba privačių patikimų institucijų siunčia signalus rinkos žaidėjams. Tame pačiame tyrime atskleista, kad taip pat pozityvus signalas siunčiamas rinkos žaidėjams, kai didelė įmonė investuoja didelę sumą į bitkoiną. Socialinės platformos tyrime [25], dėl įtakos kriptovaliutų kainai, atskleista, kad investuotojai, priimdami sprendimą investuoti ar ne, domisi ne tik kriptovaliutos istorinėmis grąžomis, tačiau ir kitais informaciniais šaltiniais, tokiais kaip socialinės platformos įrašai. Dažniausiai socialinės platformos įrašai apima vartotojo patirties pasidalinimą bei kiek sekėjų tas vartotojas turi, kokio dydžio auditorijai bus perduota sentimentų žinutė. Pastebėta, kad kriptovaliutų kainai įtaką daro socialinės platformos žinutės. Sheno atliktame tyrime [26], apie *Twitter* platformos žinučių, kuriose yra tekstas „*#bitcoin*“, daromą įtaką kriptovaliutų grąžoms, atskleista, kad kuo daugiau teksto paminėjimų yra praėjusios dienos žinutėse, tuo didesnė kriptovaliutos grąža bus kitą dieną. Taip pat pastebėta, kad kuo didesnė grąža vieną dieną, tuo daugiau bus *Twitter* žinučių su tekstu „*#bitcoin*“ kitą dieną.

Twitter yra populiari platforma, kurioje gali pasisakyti įvairūs žmonės įvairiomis temomis. Elonas Muskas yra vienas iš turtingiausių žmonių, kuris nevengia pareikšti savo nuomonės *Twitter* platformoje. Pastebėta, kad po vieno ar kito pareiškimo jo profilyje, kuris susijęs su

kriptovaliutomis, kaina būtent tos kriptovaliutos keičiasi drastiškai. Ante Lennartas savo tyrime [56] pastebėjo, kad pasirodžius naujai žinutei susijusiai su kriptovaliutomis, kaina auga vidutiniškai 3% per artimiausias kelias valandas, tuomet kaina nusistovi ir krenta žemyn. Didžiausi pakylimai pastebėti tuomet, kai Elonas Muskas savo *Twitter* profilyje pasikeitė aprašymą ir prisidėjo tekstą „*#bitcoin*“. Tuomet bitkoino kaina pakilo 13,6% per 1 valandą nuo profilyje atliktų pakitimų. Taip pat Elonas Muskas parašė žinutę, kurioje pranešė, kad jo valdoma įmonė *Tesla* nusipirko bitkoinų, kurių vertė 1,5 milijardų JAV dolerių [57]. Tuomet bitkoino kaina pakilo 9,3% per pirmą valandą. Dar tyrimo metu pastebėta, kad Elonas Muskas komunikuoja žinutę apie bitkoiną tuomet, kai jo kaina yra šiek tiek smukusi žemyn. Taip pat pastebėta, kad po jo žinutės paskelbimo, bitkoino kaina pakyla vidutiniškai 45 minutėms. Taigi Elon Musk žinutės daro teigiamą įtaką bitkoino kainai.

Garrattas Rodney ir Neila Wallace teigia [4], kad bitkoinas yra vertinimas šiandien su intencija, kad aplinkiniai jį vertins taip pat arba geriau ateityje. Šiomis dienomis neretai bitkoinas yra palyginimas su auksu. Ladislavas Kristoufekas ir Brianas Lucey [5] išskiria 4 požymius, kodėl bitkoinas yra tapatinamas su auksu. Visų pirma, tiek auksas, tiek bitkoinas yra reguliuojami kaip produktai, ypač JAV kur bitkoinas yra klasifikuojamas kaip produktas. Antra, nėra centrinės institucijos, kuri galėtų kontroliuoti aukso ir bitkoino kasybą ar jų sandorius, todėl abu nėra priklausomi nuo infliacijos. Trečia, abu yra gaminami procese, kuris vadinamas „kasyba“. Taip pat tiek aukso, tiek bitkoino ištekliai yra riboti – negalima iškasti daugiau nei 21 milijono bitkoino monetų. Ir ketvirta, pasaulio naujienos daro įtaką tiek aukso, tiek bitkoino kainai. Bauras savo darbe [27] teigia, kad plačiai paplitusios kalbos, jog bitkoinas yra naujasis auksas, ar virtualus auksas ar „auksas 2.0“ leidžia suprasti, jog bitkoinas ir auksas yra ganėtinai panašūs. Tiksliau būtų teigti, kad investuotojai vertina tiek auksą, tiek bitkoiną panašiai, todėl jų kainos turėtų koreliuoti. Tačiau Bauro atliktas tyrimas, kuriame jis naudojo įvairias koreliacijas, parodė, kad koreliacija tarp aukso ir bitkoino yra beveik nulinė.

Bitkoino tyrimai parodo, kad bitkoinas yra panašus į auksą, tačiau kartu ir skiriasi. Bitkoinas daugelio yra vertinamas kaip virtualus auksas todėl, kad bitkoino kaina nėra veikiama infliacijos bei bitkoino monetų skaičius yra ribotas, tačiau socialinės platformos įtaka yra ganėtinai didelė, todėl išlieka galimybė manipuliuoti bitkoino kaina.

1.6. Ekonominės veiklos rūšys bei bitkoino naudojimas

Ekonominėje veikla yra skirstoma į keletą rūšių. Kiekviena ekonominės veiklos rūšis atspindi skirtingą veiklą pagal jos pobūdį. Ekonominės veiklos rūšies klasifikatorių parengia Eurostatas [79]. Veiklos yra skirstomos pagal sekciją, skyrių, grupę, klasę bei poklasį. Žemiau pateiktoje lentelėje yra pateiktos ekonominės veiklos rūšys suskirstytos pagal sekciją.

1 lentelė. Ekonominės veiklos rūšių klasifikacija pagal sekciją [79]

Ekonominės veiklos rūšis	Sekcijos kodas
Žemės ūkis, medžioklė, miškininkystė, žuvininkystė	A
Kasyba ir karjerų eksploatavimas	B
Apdirbamoji gamyba	C
Elektros, dujų ir garo tiekimas	D
Vandens tiekimas	E
Statyba	F
Didmeninė ir mažmeninė prekyba; variklinių transporto priemonių ir motociklų remontas, asmeninių ir namų ūkio reikmenų taisymas	G
Viešbučiai ir restoranai	H
Transportas, sandėliavimas ir ryšiai	I
Finansinis tarpininkavimas	J
Nekilnojamasis turtas, nuoma ir kita verslo veikla	K
Viešasis valdymas ir gynyba; privalomasis socialinis draudimas	L
Švietimas	M
Sveikatos priežiūra ir socialinis darbas	N
Kita komunalinė, socialinė ir asmeninė aptarnavimo veikla	O
Privačių namų ūkių veikla	P
Žmonių sveikatos priežiūra ir socialinis darbas	Q
Meninė, pramoginė ir poilsio organizavimo veikla	R
Kita aptarnavimo veikla	S
Namų ūkių, samdančių darbininkus, veikla	T
Eksteritorialinių organizacijų ir įstaigų veikla	U

Šios ekonominės veiklos atspindi skirtingas veiklas, kuriose naudojama piniginė valiuta. Piniginė valiuta naudojama veiklose siekiant įvertinti paslaugą ar prekę ir naudojama mainais už suteiktas paslaugas ar prekes. Piniginės valiutos yra kontroliuojamos finansinių šalies institucijų, kuomet yra valdoma valiutos vertė bei kiekis cirkuliacijoje. Bitkoinas, kitaip nei piniginė valiuta, yra nepastovus bei jo kaina kinta labai greitai.

Vos tik atsiradus bitkoinui buvo manyta, kad laikui bėgant elektroninės valiutos pakeis įprastą piniginę valiutą. Tam buvo pradėta vertinti bitkoiną kaip piniginės valiutos atitikmenį. Tačiau pradėjus analizuoti bitkoino plataus naudojimo galimybes susidurta su tam tikrais klausimais bei iššūkiais [81]. Pastebėta, kad bitkoinas prastai funkcionuoja kaip apskaitos vienetas. Visų pirma, bitkoino kaina kinta labai greitai. Kintanti bitkoino kaina turi įtakos vykdomoms transakcijoms bitkoino blokų grandinėje bei jų patvirtinimo greičiui ir mokesčio dydžiui. Antra, bitkoino transakcijų skaičius per dieną yra daug mažesnis nei įprastos piniginės valiuotos. Bitkoino blokų grandinėje per dieną yra įvykdomos 631 677 transakcijos [2023-05-15 duomenimis] [82]. 2018 metų duomenimis per dieną vidutiniškai atliekamos 1.01 milijardo transakcijų naudojant įprastą piniginę valiutą [83]. Vadinasi, net po 5 metų, bitkoinas nepralenkė įprastų piniginių valiutų transakcijų skaičiumi per dieną. Tai rodo, kad bitkoino panaudojimas vietoje piniginės valiutos yra limituotas.

Viena iš priežasčių, kodėl buvo pradėta abejoti šia idėja, yra tai, kad elektroninės valiutos kaina nėra reguliuojama finansinių institucijų. Vadinasi, kaina gali ženkliai svyruoti [80]. Kaip alternatyva, atsirado bitkoino valiutos panaudojimas ekonominėse veiklose, tačiau bitkoinas buvo naudojamas ne tiesiogiai. Bitkoino monetos yra pervedamos į tarpinę mokėjimo sistemą, kuri veikia kaip keitykla ir perveda galutiniam gavėjui lėšas įprasta pinigine valiuta. Tokio tipo netiesioginis bitkoino panaudojimas yra galimas visose ekonominės veiklos rūšyse. Žemiau išvardinti apibendrinti sektoriai ekonominės veiklos rūšių, kuriuose naudojamas bitkoinas.

2 lentelė. Ekonominių veiklų rūšių klasifikacija pagal sekciją, kuriose naudojamas bitkoinas

Ekonominės veiklos rūšis	Sekcijos kodas
Statyba	F
Didmeninė ir mažmeninė prekyba; variklinių transporto priemonių ir motociklų remontas, asmeninių ir namų ūkio reikmenų taisymas	G
Viešbučiai ir restoranai	H
Transportas, sandėliavimas ir ryšiai	I
Finansinis tarpininkavimas	J
Nekilnojamasis turtas, nuoma ir kita verslo veikla	K
Švietimas	M
Meninė, pramoginė ir poilsio organizavimo veikla	R

Yra išskiriamos keletas ekonominių veiklų, kuriose bitkoinas yra naudojamas tiesiogiai kaip piniginė valiuta. Viena iš tokių veiklų yra statyba. Statant naujus būstus, statytojai siekia kuo greičiau rasti pirkėjus bei palengvinti jiems atsiskaitymo procesą, kad pinigai greičiau atsidurtų statytojų sąskaitoje ir turtą būtų galima įsigyti lengviau. Didžiausi privalumai perkant būstą bitkoinais yra tai, kad lėšos yra pervedamos greitai bei transakcijos mokesčiai yra mažesni. Taip pat yra daug lengviau atsiskaityti su užsienio šalių statytojais, kadangi nereikia mokėti papildomų mokesčių dėl tarptautinių pavedimų bei nereikia ilgai laukti, kol bankai patvirtins bei įvykdys transakcijas. Kitas pliusas yra tai, kad negalima atšaukti transakcijų bei lėšos pervestos į gavėjo piniginę, negali būti atšauktos, tai gali padaryti tik pats pardavėjas. Jeigu būsto statytojai priima atsiskaitymus bitkoino monetomis, tuomet galima pritraukti didesnius investuotojus, kurie yra turtingesni bei dažniausiai jie nori turtą įsigyti pakankamai greitai bei nemokant didelių mokesčių [85].

Kita labiausiai paplitusi bitkoino naudojimo ekonominė veikla yra sektorius G – didmeninė ir mažmeninė prekyba. Šis sektorius yra labai platus bei jis apima visokias prekybos rūšis. Dažniausiai tokiose prekybos vietose negalima atsiskaityti tiesiogiai bitkoino monetomis, bet galima naudoti tarpinę finansinę platformą, kurios veikia kaip bitkoino keityklose, ir tuomet galima atsiskaityti už įvairias prekes ar paslaugas [86]:

- prekės *Amazon* tinklalapyje,
- *Apple* produktai,
- knygos,
- bilietai,
- automobiliai bei jų dalys,
- mobilieji telefonai,
- drabužiai,
- mados aksesuarai,
- kompiuteriniai prietaisai,
- kava,
- papuošalai,
- internetinės paslaugos,
- dronai,
- kita elektronika,
- galima aukoti nepelno siekiančioms organizacijoms,
- ir kt. paslaugos.

Sektorius H, apimantis viešbučius bei restoranus, taip pat priima atsiskaitymus bitkoino monetomis. Yra daug įmonių, tiek maisto tiekėjų, tiek viešbučių, kurie priima atsiskaitymą bitkoinais per tarpininkus, tačiau yra ne vienas prabangus bei žymus viešbutis, kuris suteikia savo klientams galimybę atsiskaityti už paslaugas ar viešbučio rezervaciją tiesiogiai bitkoinais. Tokiu atveju viešbučio administratorius atsiunčia elektroniniu laišku virtualios piniginės adresą bei pirkėjas gali atlikti transakciją [87]. Tiesioginis atsiskaitymo būdas yra labiau priimtinas pirkėjams, nes tuomet galima išvengti papildomo tarpininkavimo mokesčio.

Transporto, sandėliavimo bei ryšių ekonominės veiklos sektorius apima įvairias susisiekimo paslaugas. Oro linijos jau priima atsiskaitymą už bilietus tiesiogiai bitkoinais. 2013 metais *CheapAir* bendrovė buvo pirmoji, kuri nusprendė priimti atsiskaitymą bitkoinais [89]. 2019 metais

Norvegijos oro linijos *Norwegian Ai*r paskelbė, kad nuo šiol priiminės atsiskaitymus bitkoinais ir negana to, jie įsteigė naują bitkoinų keityklą *NBX*. Jie netgi sukūrė lojalumo programą, kuri skatino naudotis kriptovaliutomis bei jų įsteigta keitykla, tokiu būdu rinkti lojalumo taškus bei panaudoti juos atsiskaitant už bilietus [88].

Nuo 2014 metų atsirado ne vienas startuolis, kuris teikė įvairias finansines paslaugas susijusias su bitkoinu: kriptovaliutų piniginių tiekėjai, bitkoino keityklos, mokėjimų apdorojimo platformos, finansinių paslaugų tiekėjai, kasėjai ir universalūs paslaugų tiekėjai, kurie turi visas išvardintas paslaugas vienoje platformoje [84]. Šios visos ekonominės veiklos patenka į sektorių J – finansinis tarpininkavimas.

Nekilnojamasis turtas, nuoma ir kita verslo veikla yra kitas sektorius, kuriame priimamas bitkoinas kaip piniginė valiuta. Tam tikros nekilnojamo turto brokerių agentūros nusprendė priimti atsiskaitymą bitkoinais, kadangi tai padeda pritraukti turtingesnius klientus bei bitkoinas yra pritaikytas atsiskaitymams didelėmis sumomis. Lengviausias būdas tai padaryti yra pasinaudoti tarpinėmis platformomis, kurios konvertuoja bitkoinus į įprastą valiutą. Jei nekilnojamo turto bendrovė priima atsiskaitymus bitkoinais tiesiogiai, tuomet bendrovė rizikuoja mokėti didesnius mokesčius, kai norės išsigryninti bitkoinus į įprastą piniginę valiutą. Antra, nėra galimybių patikrinti iš kur yra gautos lėšos pirkėjo sąskaitoje, ar jos nėra susijusios su įtartinomis , nelegaliomis veiklomis. Trečia, bitkoino kaina kinta greičiau nei įprastos valiutos [90]. Nepaisant šių sunkumų, nekilnojamo turto rinkoje yra įmonių, kurios priima atsiskaitymus tiesiogiai bitkoinais.

Švietimas yra kita ekonominė veikla, kurioje galima atsiskaityti bitkoinais. 2014 metais Kumbijos universitetas (angl. *Cumbia University*) paskelbė, kad priims mokėjimus bitkoino valiuta iš studentų, kurie mokysis su kriptovaliutomis susijusią magistro studijų programą [91]. Viena iš žinomiausių technologijų įmonių Microsoft priima mokėjimus bitkoinais nuo 2014 metų [92]. Tiek universitetai tiek Microsoft neteikia galimybės atsiskaityti tiesiogiai bitkoinais, todėl norintys mokėti bitkoinais turi naudotis tarpininkų paslaugomis.

Kita ekonominė veikla yra labiausiai paplitusi kriptovaliutų atsiskaitymuose. Meninės ekonominės veiklos sektorius tapo labai populiarus kriptovaliutose. Atsiradus bei išpopuliarėjus kriptovaliutai, buvo pradėti kurti elektroniniai meno kūriniai – nekeičiami žetonai (angl. *Non Fungible Tokens* (*NFTs*)). Šie nekeičiami žetonai yra skaitmeniniai meno kūriniai. Kai įsigyjamas tokio tipo meninis kūrinys, tuomet pirkėjas gauna skaitmeninę laikmeną su meno kūriniu bei paštu gauna jo originalą [93].

Aptartos 8 ekonominės veiklos rūšys, kuriose naudojamas bitkoinas bei vykdomi atsiskaitymai šia kriptovaliuta. Šios ekonominės veiklos parodo, kad bitkoinas yra tinkamas ir naudojamas kasdieniuose atsiskaitymuose, tačiau neretai yra naudojama tarpinė sistema, kuri apdoroja bitkoino mokėjimus.

1.7. Sukčiavimo atvejai naudojant kriptovaliutas

Sukčiavimo atvejų pasitaiko kiekvienoje valiutoje. Kai atsirado bitkoinas ir po truputį pradėjo populiarėti, piktavaliai vartotojai surado naują būdą kaip apgaudinėti. Bitkoinas daugelį sužavėjo savo anonimiškumo savybe. Ilgą laiką buvo manyta, kad bitkoino transakcijų savininkų negalima atsekti, kadangi sukurti virtualią piniginę yra taip paprasta ir šis procesas nereikalauja jokių asmens

duomenų pateikimo ar jų patvirtinimo. Remiantis šia savybe, anoniminiai sukčiai ėmėsi darbo. Irwinas ir Turneris mano [15], kad kriptovaliutų sistema yra ganėtinai palanki sukčiavimams bei pinigų plovimui lyginant su įprasta, tradicine pinigų sistema. Ypač todėl, kad nėra renkama asmeninė informacija apie klientus.

Vienas iš didžiausių skandalų kriptovaliutose buvo bitkoino naudojimas siekiant paveikti 2016 metų JAV prezidento rinkimus. Rusija naudojo bitkoino kriptovaliutą beveik kiekviename žingsnyje stengdamasi paveikti amerikiečių nuomonę balsavime [29]. Buvo naudojamasi internetinėmis sistemomis, kurios buvo apmokėtos bitkoinais, kad nulaužti demokratų partijos sistemas ar internetines paslaugas, tuomet buvo paskelbtas dezinformacijos turinys, siekiant paveikti amerikiečių nuomonę. JAV institucijų atliktame tyrime nustatyta, kad didžioji dalis dezinformacijos kampanijų buvo įvykdyta Rusijos internetinių paslaugų dėka. Tyrime teigiama, kad piktavaliai prisidengdavo netikromis ar pavogtomis tapatybėmis ir dažnai naudojo tą patį kriptovaliutų piniginės adresą, tuomet buvo lengviau atsekti pinigines, kurios susijusios su šiomis transakcijomis. JAV institucijos paviešino visą tyrimą bei bylą, kurioje galima rasti įvykdytas transakcijas ir piniginių adresus, kurios dalyvavo nelegalioje veikloje. Straipsnyje [29] teigiama, kad sukčiai įsibraudavo į amerikiečių asmeninius kompiuterius, o tam buvo panaudotos lėšos bitkoinais, kurių suma buvo apie 95 000 JAV dolerių.

Norint užkirsti kelią pinigų plovimui, Europos Sąjunga 2018 metais išleido 5 direktyvą prieš pinigų plovimą, kuris įgalino įrankius, kurie padeda surasti ir užkirsti kelią pinigų plovimo schemoms bei terorizmo finansavimui naudojant kriptovaliutas. Tais pačiais metais Europos Sąjunga skyrė didesnį dėmesį nacionaliniam finansinių operacijų tyrimų biurui, kad jie išspręstų kriptovaliutų anonimiškumo riziką ir turėtų galimybę gauti informaciją apie virtualių kriptovaliutų piniginių savininkus bei juos identifikuoti [30].

Bitkoinas viena iš populiariausių kriptovaliutų iki šiol. Ypatingai paskutiniu metu bitkoino kaina vis kilo ir kilo aukštyn, todėl nenuostabu, kad yra norinčių pasipelnyti iš to bei naudoti bitkoinus nelegalioje veikloje. Yra skirtingų sukčiavimų būdų, vieni populiariausių yra *Ponzi* schemos, kėsinimaisi nulaužti bitkoino keityklas ar kitas kriptografinių valiutų keityklas, apgaulės išgaunant bitkoiną iš privačių asmenų bei šantažuojantys elektroniniai laiškai [21].

Vienas iš būdų yra taip vadinamos *Ponzi* schemos [22]. Šios internetinės platformos suvilioja vartotojus siūlydamos neįprastai dideles palūkanas, kurios gali siekti netgi 2% dienos grąžos. Naujos platformos stengiasi pritraukti kuo daugiau vartotojų, todėl pirmieji vartotojai gauna išmokas, tačiau kiti vartotojai, patikėję savo lėšas, gali jų ir nebeatgauti. Dažniausiai šios platformos yra greitai atsekamos, todėl kad kriptovaliutų savininkai domisi tokiomis platformomis, skelbia apie jas forumuose, todėl po neigiamų patirčių tokios platformos praranda staigų populiarumą ir užsidaro. Tačiau tie patys platformų kūrėjai atidaro naują platformą, kuri veikia tokio pačiu principu, bei bando privilioti naujus vartotojus prisidengę kitu vardu. Blokų grandinė savo savybėmis yra labai patraukli *Ponzi* schemų veiklai, todėl kad kriptovaliutų pinigines galima sukurti be asmens identifikavimo bei atliktų transakcijų nebegalima atšaukti.

Elektroniniai laiškai, su šantažuojančiu turiniu, būna patys įvairiausi. Dažniausiai susisiekiama su auka ir pranešama, kad galimai į jų kompiuterį ar telefoną buvo įsilaužta ir sukčiautojai dabar turi svarbios asmeninės informacijos, todėl auka turi pervesti tam tikrą bitkoinų sumą į kriptovaliutų

piniginę [21]. Tokiu būdu šantažuojantys asmenys neprašo didelės sumos, kad žmonės patikliau reaguotų bei atliktų transakciją.

Bitkoino keityklų nulaužimas yra kitokio pobūdžio sukčiavimas, kadangi tada atakuojamas ne asmuo, o keitykla ir yra didesnė tikimybė gauti didesnę kriptovaliutų sumą. Kriptovaliutų keityklų serverių nulaužimas yra ganėtinai dažnas reiškinys. Pirmoji ataka įvyko praėjus keliems metams po bitkoino atsiradimo, 2012 metais, kovo 1 dieną, kuomet buvo įsilaužta į *Bitcoinica* keityklą ir keityklos nuostolių dydis siekė 87 000 JAV dolerių [28]. 2014 metais Wagstaffas ir Karpeles pranešė [14] apie vieną didžiausių bitkoinų vagysčių bitkoino keitykloje *MT Gox*. 2014 metų vasario mėnesį bitkoinų keitykla neteko 850 000 bitkoinų, kurių vertė tuo metu siekė 450 mln. JAV dolerių. Dar didesnis nuostolis buvo patirtas *CoinCheck* keitykloje, kuomet 2018 metais sausio 27 dieną buvo pavogta 560 mln. JAV dolerių. Na, o pats didžiausias nuostolis buvo patirtas *FTX* keitykloje 2022 metais, kuomet buvo pavogta net 600 mln. JAV dolerių vertės kriptovaliutų. Viena iš blokų grandinę tiriančių įmonių *CipherTrace* pateikė raportą, kuriame teigiama, kad 2020 metų pavasario duomenimis globaliai pinigų plovimo operacijos buvo panaudota bitkoinų už 4,5 mlrd. JAV dolerių. Dauguma bitkoino transakcijų (74%) buvo lėšos, kurios keliavo iš vienos bitkoinų keityklos į kitą. Tai tik įrodo, kad bitkoinų keityklos turėtų rūpintis pinigų plovimo prevencinėmis programomis ir jų analizėmis [16].

Visi šie sukčiavimo atvejai yra panašūs tuo, kad turi bendrą tikslą – apgauti auką, surinkti lėšas bei likti nepastebėtiems. Nors naudojami ir skirtingi metodai bandant sukčiauti blokų grandinėję, tačiau veiksmai yra ganėtinai panašūs. Tiek privačių asmenų, tiek bitkoinų keityklų sukčiavimo atvejais yra naudojamos panašios schemos. Visų pirma, bandoma išvilioti pinigus iš keityklos ar privačių asmenų, tuomet, bandoma atlikti daug įvairiausių transakcijų, kad paslėpti pėdsakus ir, tuomet, pervedamos lėšos į vieną piniginę, su kuria bandoma išgryninti bitkoinus į piniginę valiutą, arba išskirstomos lėšos per kelias kriptovaliutų pinigines ir bandoma išgryninti apgaulės būdu gautus pinigus po truputį.

Tiriant blokų grandinę bei bandant atrasti sukčiavimo atvejus, svarbu suprasti bitkoino anonimiškumą. Bitkoinas yra anonimiška valiuta, jeigu naudojamos kriptovaliutų piniginės ir pinigai nėra pervedami į bitkoinų keityklas. Jei pinigai pasiekė keityklą, jau galima identifikuoti, kas yra piniginės savininkas. Jeigu transakcijos vykdomos iš vienos piniginės į kitą nenaudojant bitkoinų keityklos, išlikti anonimišku yra ganėtinai paprasta. Kai kurios kriptovaliutų piniginės yra paviešintos, todėl jas galima identifikuoti, tačiau naują piniginę susikurti užtrunka tik keletą minučių, todėl savininkai neretai turi ne vieną kriptovaliutų piniginę.

Gaihre, Luo ir Liu [17] išskiria keturias pagrindines deanonimizacijos kryptis. Pirma, sekti bitkoino savininkus bei jų veiksmus. Šiais laikais yra platformos, tokios kaip *HelixMixer, Coinjoin*, kurių dėka galima sumaišyti esamus bitkoinus ir gauti naujus, kaip jie teigia, „švarius“ bitkoinus. Tokios „sumaišymo“ platformos veikia tokiu principu, kad norintys išlikti anoniminiais asmenys siunčia savo lėšas į vieną iš platformų, tuomet tos lėšos yra maišomos su kitų vartotojų lėšomis bei atlikus daugybę įvairiausių skaidymo bei stambinimo monetų transakcijų yra ganėtinai sudėtinga atsekti iš kur atkeliavo tie bitkoinai [58]. Antra, naudojant įrankius, kaip *Bitlodine*, atviro kodo blokų grandinės analitikos įrankius, galima automatiškai surinkti bei atnaujinti sąrašą bitkoino piniginių, kurių savininkai yra žinomi. Trečia, naudotis bitkoino klientų programine įranga, kuri padeda atpažinti piniginių adresus bei jų savininkus. Ketvirta, analizuoti bitkoino transakcijų grafus. Meiklejohn savo darbe [18] grupavo bitkoino pinigines bandydama klasifikuoti su sukčiavimu

susijusius bitkoino piniginių adresus. Kiti tyrime bandė analizuoti bitkoino transakcijų grafus, siekiant atsekti transakcijas, susijusias su bitkoino vagystėmis ar sukčiavimu [19]. Taip pat transakcijų grafams buvo pritaikyti mašininio mokymosi metodai, siekiant apmokyti modelį atrasti įtartinas grafo struktūras [20].

1.8. Blokų grandinės tyrimai siekiant atrasti sukčiavimo atvejus

Yra atliktas ne vienas tyrimas siekiant ištirti blokų grandinę bei bitkoino transakcijas. Viena iš bitkoino savybių – anonimiškumas. Neretai šią savybę bandoma paneigti, siekiant atrasti ryšius tarp anoniminių transakcijų bei tų transakcijų gavėjų, bandoma juos identifikuoti. Tyrimuose bandoma atrasti sąsajas, kurios padėtų identifikuoti įtartinas transakcijas, įtartinas pinigines. Dažniausiai tyrimuose naudojami įvairūs mašininio mokymosi metodai, kurių metu modelio treniravimui pateikiamos tam tikros transakcijos, kurios jau yra identifikuotos kaip įtartinos, tai gali būti jau paskelbtų valstybinių institucijų tyrimų rezultatai ar viešai identifikuotos piniginės ar transakcijos. Kiti autoriai savo tyrimuose naudoja grafinius transakcijų tyrimo metodus, kurių metu analizuojami grafai bei identifikuojamos įtartinos transakcijos. Vėlgi, dažnai modelio treniravimui naudojami duomenys, kurie yra pateikti oficialių šaltinių bei patvirtinti.

Gaihre savo tyrime [17] tyrė bitkoino transakcijas bei virtualių piniginių adresus. Tyrime naudoti duomenys apėmė bitkoino transakcijas, nuo bitkoino atsiradimo iki 2018 metų. Buvo analizuojamos transakcijos bei sudaromi grafai siekiant išsiaiškinti ar vartotojams yra svarbus bitkoino anonimiškumas. Analizuojant transakcijų grafus buvo lyginamos keturios pagrindinės grafo charakteristikos:

- Sujungti komponentai (angl. *connected component undirected graph*), kuriuose kiekviena viršūnė gali pasiekti kitas viršūnes. Šiame analizės žingsnyje siekiama surasti sujungtų komponentų skaičių bitkoino transakcijų grafe.
- Grafo skersmens suradimas. Grafo skersmuo yra ilgiausias kelias iš visų trumpiausių grafo kelių. Analizuojamas grafas turi 720 milijonų viršūnių bei 3.38 milijardų briaunų, todėl norint paskaičiuoti grafo skersmenį, tai užtruktų ganėtinai ilgai, todėl tyrime naudojamas apytikslis grafo skersmens įvertis.
- Grafo viršūnės laipsnio analizė. Grafo viršūnės laipsnis – briaunų skaičius vienoje viršūnėje.
- Transakcijų įvesčių analizė. Svarbu atkreipti dėmesį į transakcijų įvesčių vertę, kokios sandorių sumos bei kokios sumos pasiekia vieną ar kitą virtualią piniginę.

Tyrimo metu buvo bandoma atsakyti į klausimą – ar bitkoino vartotojams svarbu bitkoino anonimiškumas? Rezultatai parodė, kad jeigu transakcijų suma yra ganėtinai maža, tuomet bitkoino vartotojai nėra susirūpinę bitkoino anonimiškumu, tačiau jeigu sumos yra ženkliai didesnės, tuomet vartotojai nori išlikti anonimiški.

Kitas tyrimas atliktas Yan Wu [31] bandė paaiškinti bitkoino transakcijas, kurios susijusios su pinigų plovimo schemomis. Buvo siekiama, kad šio tyrimo metu, sukurtas modelis atpažintų Šilko kelio transakcijas. Šio tyrimo metu yra naudojamos 19 charakteristikų apie bitkoino transakcijas:

- transakcijos laikas,
- transakcijos įvesčių skaičius,
- transakcijos išvesčių skaičius,
- transakcijos įvesčių adresų skaičius,

- transakcijos išvesčių adresų skaičius,
- transakcijos įvesties vertė,
- kiek kartų piniginės adresas pasikartoja transakcijos išvestyse,
- kiek kartų piniginės adresas pasikartoja transakcijos įvestyse,
- adresų išvesčių skaičius,
- pirmos transakcijos laikas,
- paskutinės transakcijos laikas,
- skaičius įvesties adresų, iš kurių pervedami pinigai į vieną adresą,
- skaičius išvesties adresų, į kuriuos pervedami pinigai iš vieno adreso,
- bitkoino vertė transakcijos įvestyje,
- ar lėšos yra naudojamos kitoje transakcijoje,
- piniginės lėšų likutis,
- gauta pinigų suma į vieną adresą iš viso,
- balanso monetų genas (naudojamas sekti pirmutinių transakcijų monetoms bei joms identifikuoti),
- gautų monetų genas (naudojamas sekti norimos analizuoti transakcijos monetoms).

Šio tyrimo metu buvo nagrinėjamos senesnės bitkoino transakcijos, kurios buvo susietos su *Mt. Gox* bitkoino keitykla, iš kurios 2014 metais buvo pavogti apie 500 milijonų bitkoinų. 2014 metais buvo paviešinti adresai bei transakcijos iš bei į *Mt. Gox* keityklą, tačiau ši informacija nebėra prieinama viešai. Sukčiavimo modelis truko ne vienus metus. Bitkoinai buvo pervedami į kitas pinigines, kuriose buvo kaupiamos lėšos bei vėliau skaidomi į kitas pinigines ir lėšos buvo pervedamos į keityklas, iš kurių lėšos buvo išgrynintos. Šio tyrimo metu autoriai naudojo *Mt. Gox* keityklos adresą bei bandė atsekti transakcijas susijusias su šiuo adresu. Rezultate modelis išskyrė transakcijas, kurios atitiko 7 požymius dėl galimo sukčiavimo:

1. Ne mažiau nei trys įvesčių adresai transakcijoje, kurioje lėšos pervedamos į didesnę, apjungiančią piniginę.
2. Kiekviena apjungianti piniginė balanse turi pora tūkstančių bitkoinų.
3. Transakcijos yra fiksuotos nuo 2011 metų liepos mėnesio.
4. Kiekviena transakcija į apjungiančią piniginę turi tik vieną išvestį.
5. Išvesčių adresų skaičius yra ne mažesnis nei 2.
6. Iš apjungiančios piniginės lėšos buvo pervedamos tik į vieną piniginę.
7. Transakcija turi turėti seniau minėtą transakcijos gautų monetų geną.

Šis modelis rezultate atrinko 236 piniginių adresus, kurioms buvo pervesti 560 tūkstančiai bitkoinų, tai parodo, kad šis metodas yra ganėtinai veiksmingas atrenkant įtartinas bitkoino transakcijas, tačiau šiame metode reikia turėti užuominas ar įtartinų piniginių adresus nuo kurių galima būtų pradėti tyrimą. Jeigu žinomas bent vienas piniginės adresas, galima būtų tirti transakcijas, kurios susijusios su ta pinigine, naudojant šį metodą.

Kitas tyrimas, kuris analizavo bitkoinų transakcijas bei sukčiavimo atvejus juose, yra atliktas Lorenzo [33] bei jo metu buvo naudojamas mašininis mokymasis be mokytojo. Šio tyrimo metu buvo naudojamas *Ellicit* įmonės parengtas duomenų rinkinys, kuris apėmė 49 grafus, iš viso apie 200 000 transakcijų iš kurių 21% sudaro transakcijos, kurios yra iš keityklų, iš kasėjų ar kitų oficialių šaltinių, 2% duomenų rinkinio sudaro transakcijos, kurios yra susijusios su sukčiavimu, apgavystėmis, terorizmu, įtartinomis organizacijomis ar *Ponzi* schemomis, ir visos kitos

transakcijos, kurios gali būti įvairios. Kiekviena transakcija turi 166 savybes, iš kurių 94 savybės sudaro informacija apie transakcijas, likusios savybės yra suskaičiuojamos sudarant grafus. Šio tyrimo metu didžiausias iššūkis buvo klasių disbalansas, kadangi tik 2% transakcijų yra susijusios su sukčiavimu, tai ganėtinai maža duomenų rinkinio dalis. Taip pat tyrime buvo išbandyti keli skirtingi mašininio mokymosi metodai bei geriausiu išrinktas atsitiktinių miškų metodas.

Kadangi bitkoino įtartinų transakcijų slėpime yra populiaru naudoti „sumaišymo“ tinklalapius, buvo atliktas tyrimas, kuris siekė atrasti tokias sumaišytas transakcijas. Sun [59] savo tyrime bandė atrasti metodą, kuris padėtų atpažinti bitkoino monetų sumaišymo transakcijas. Šiame tyrime buvo sukurtas mašininio mokymosi metodas paremtas giluminiu mokymusi, kuris sugebėjo atrasti naujas klases bei identifikuoti sumaišytas transakcijas geriau nei taisyklių pagrindu grįsti mašininiai mokymaisi. Duomenų rinkinys buvo sudarytas iš 132 480 bitkoino monetų sumaišymo transakcijų iš 270 000 – 300 000 blokų. Senesni blokai pasirinkti todėl, kad anksčiau sumaišymo algoritmai buvo paprastesni, nes dar nebuvo tokie populiarūs. Duomenys buvo padalinti į dvi imtis – viena modelio treniravimui, kurioje buvo senesnės transakcijos su lengvai aptinkamomis sumaišymo transakcijomis bei jos buvo pažymėtos atitinkamai, bei kita imtis skirta modelio testavimui. Antroje imtyje duomenys buvo naujesni bei transakcijos buvo sudėtingesnės. Šio tyrimo metu tikėtasi, kad modelis, išmokęs atpažinti sumaišymo transakcijas ankstesnių metų transakcijose, sugebės atpažinti panašius algoritmus ir naujesniuose duomenyse. Tyrimo rezultatuose aptariama, kad nėra lengva atpažinti sumaišymo transakcijas automatiniu taisyklių metodu, dažnai prireikia žmogaus sprendimo bei įvertinimo, todėl, norint pasiekti geresnį modelio tikslumą ir tobulinant modelį, tikslingiau būtų turėti didesnį kiekį transakcijų, kurios yra pažymėtos kaip sumaišymo transakcijos.

Francesco Maesa [60] savo tyrime taip pat nagrinėjo bitkoino transakcijų grafus. Šiame tyrime buvo siekiama priskirti grafus klasteriams pagal piniginių adresų savininkus. Vadovautasi taisykle, kad kiekvienam x ir y, jeigu egzistuoja transakcija (A_1, A_2) kur x, y priklauso A_1, tuomet x ir y priklauso tam pačiam klasteriui. Kita taisyklė teigia, kad jeigu x ir z priklauso A_1, kai transakcija $(A_1, A_2) \in T$ ir z, y priklauso A_3 bei transakcijai $(A_3, A_4) \in T$, tada x, y, z bus tame pačiame klasteryje. Tyrime naudotos transakcijos iki 389 799 bitkoino bloko. Taip pat šiame tyrime buvo atsižvelgta į „turtingas tampa turtingesniu“ hipotezę. Tyrimo autorė teigia, kad tikrinama hipotezė apie turtingumą kuomet vartotojas yra turtingas, jeigu jo sąskaitos balansas arba transakcijos suma yra ženkliai didesnė lyginant su kitų vartotojų. Tyrimo metu pastebėta, kad daugiau grafo viršūnių yra tuomet, kai transakcijos suma yra tarp 0.00001 ir 0.0001 bitkoino. Kai transakcijos suma viršija vieną bitkoiną, tuomet transakcijų grafo viršūnių skaičius yra mažesnis. Rezultate pastebėta, kad „turtingas tampa turtingesniu“ savybė bei centrinės grafo viršūnės yra susiję. Turtingesni vartotojai tampa kaip centrai kitoms transakcijoms. Taip pat šiame tyrime paaiškėjo, kad centrinės grafo viršūnės yra susijusios su turtingesnių piniginių savininkais.

Apibendrinant galima teigti, kad yra atliktas ne vienas tyrimas, kuris bando paaiškinti bitkoino transakcijų veiklą, atpažinti galimus sukčiavimo atvejus. Daugumoje tyrimų yra naudojamas nedidelis duomenų kiekis, pasirenkama atitinkama duomenų imtis, kuri yra gauta pasitelkiant išorinius šaltinius. Tokiu būdu yra kuriami mašininio mokymosi metodai, kadangi yra sudaryta tinkama imtis modelio treniravimui. Kitu atveju naudojamos bitkoino transakcijos, kurios priklauso senesniems blokams. Tokiu atveju siekiama sudaryti modelį, naudojantis senesniais duomenimis, bet tikimasi, kad modelis bus tinkamas ir naujesniems duomenimis. Analizuojant literatūrą pastebėta, kad dauguma tyrimų yra susiję su sukčiavimo atvejų atpažinimu, tačiau yra nedaug

literatūros, kuri bandytų paaiškinti bitkoino transakcijas bei priskirti jas ekonominėms veikloms. Bitkoino naudojimas yra plačiai paplitęs, todėl didžioji dalis ekonominių veiklų jau yra suteikę galimybę atsiskaityti naudojantis bitkoinu. Didžiausias dėmesys lieka sukčiavimo atvejų atpažinimui. Taigi, atsižvelgiant į šių atliktų tyrimų rezultatus, keliu tokias užduotis: sudaryti bitkoino transakcijų grafus, kurie apimtų prieš tai buvusias transakcijas, sudaryti galutinį duomenų rinkinį, kuriame būtų tiek grafų savybės tiek informacija apie transakcijas, pritaikyti matematinius metodus bei klasifikuoti transakcijas, sudaryti transakcijų vertinimo koeficientą, tuomet priskirti transakcijas ekonominėms veikloms bei įvertinti sukčiavimo atvejų galimybę.

2. Bitkoino transakcijų tyrimo metodika

Šiame skyriuje aptariamas bitkoino transakcijų duomenų rinkinio pasiruošimas, patirti iššūkiai bei problemos. Paaiškinami bitkoino transakcijų klasterizavimo metodai. Aptariami naudojami metodai bitkoino transakcijų grafo vaizdavimui.

2.1. Duomenų rinkinio pasiruošimo iššūkiai

Daugumoje atliktų bitkoino tyrimų naudojami jau iš anksto paruošti duomenų rinkiniai. Viename tyrime [1] buvo naudojamas duomenų rinkinys, kuris turi blokus nuo 1 iki 464 383, tai atitinka bitkoino blokus nuo jo atsiradimo 2009 metų sausio 3 dieną iki 2017 metų gegužės 1 dienos. Kadangi šiame transakcijų tyrime norėta naudoti tiek senesnius, tiek naujesnius blokus, tai šis duomenų rinkinys netiko. Taip pat naudojantis šiuo duomenų rinkiniu būtų sudėtingiau atsekti transakcijas iki pačios pirminės, kadangi nežinome, kuriame būtent bloke yra buvusioji transakcija. Tokiu atveju reikėtų kurti algoritmą, kuris kas kartą kreiptųsi į visus duomenų rinkinyje esančius blokus, tai galimai užtruktų daug daugiau laiko. Panašūs iš anksto paruošti duomenų rinkiniai naudojami daugelyje tyrimų, tačiau jie labiau tinkami tiriant transakcijas, esančias viename bloke, bei norint analizuoti pavienes transakcijas bei jų savybes.

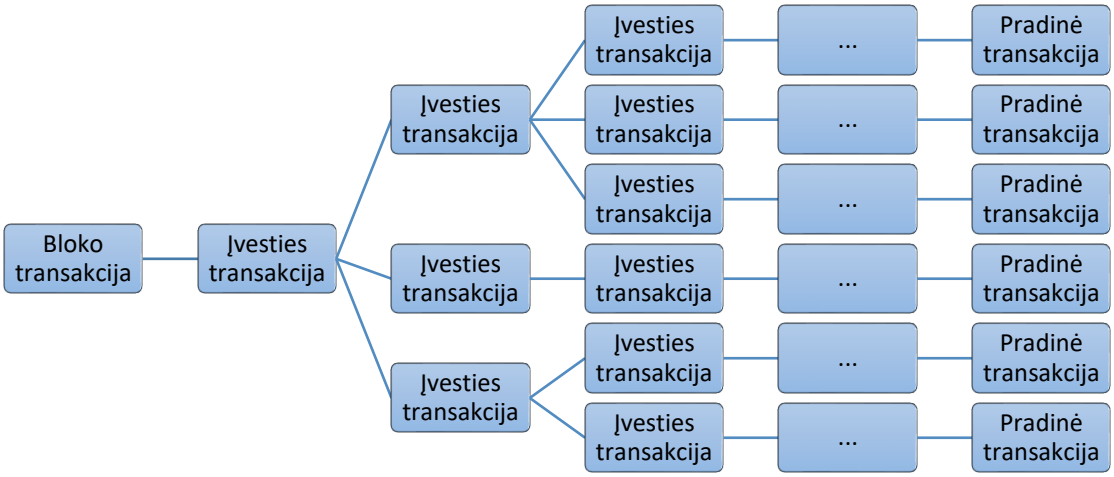
Kitame tyrime [2] naudotas duomenų rinkinys yra parengtas *Elliptic* įmonės, kuri dirba ties nusikalstamų veiklų atpažinimu kriptovaliutose. Šis duomenų rinkinys turi grafų viršūnes ir kraštines, kurie parengti pagal bitkoino blokų grandinės duomenis. Šis duomenų rinkinys viso turi 203 769 transakcijas. Dėl ganėtinai ribotos informacijos, kuri pateikiama šiame duomenų rinkinyje, šio duomenų šaltinio buvo atsisakyta. *Elliptic* įmonė turi ir kitokius duomenų rinkinius, tačiau jie nėra prieinami viešai ir nemokamai. Šios įmonės duomenų rinkiniai turi privalumą, kadangi jie gali atrinkti bei pateikti atskirai pažymėtas įtartinas transakcijas, kurios yra susietos su nusikalstama veikla, todėl taikant mašininį mokymą, tokios transakcijos padeda modeliui mokytis.

Atliekant bitkoino transakcijų tyrimą buvo išbandyti keli duomenų gavimo variantai. Iš pradžių buvo svarstyta naudoti viešai prieinamus duomenis, kurie yra patalpinti „*Google BigQuery*“. Tai yra duomenų sandėlis, kuriame yra pateikiami įvairūs duomenys bendram naudojimui. Šioje saugykloje yra duomenų rinkiniai: *bitcoin_blockchain* bei *crypto_bitcoin*. Pirmasis rinkinys *bitcoin_blockchain* turi dvi lenteles: *blocks* ir *transactions*. Šios lentelės atskleidžia bloko informaciją atitinkamai apie blokus bei apie transakcijas. Šios lentelės šiek tiek skiriasi nuo kito duomenų rinkinio *crypto_bitcoin*. Pastarąjį rinkinį sudaro taip pat dvi lentelės: *blocks* ir *transactions*, tačiau šiame rinkinyje galima rasti detalesnės informacijos apie transakcijas. Lentelėje *transactions* yra įtrauktas laukelis apie buvusios transakcijos maišą. Šis duomenų rinkinys yra prieinamas naudojantis *Google Cloud* platforma, kurioje užsiregistravus galima 60 dienų nemokamai naudotis *Google Cloud* paslauga bei vartotojui yra suteikiamas 300 JAV dolerių kreditas, kuris yra naudojamas norint vykdyti duomenų rinkinių užklausas ar išsaugoti rezultatų lenteles. Svarstant šio rinkinio tinkamumą tyrimui buvo nuspręsta, kad nemokamos versijos turėtų pakakti duomenų rinkiniui sudaryti, tačiau duomenys yra pateikti lentelės forma, todėl kurti SQL užklausą, kuri surinktų visą bitkoino transakcijų grafo informaciją nuo paskutinės transakcijos iki senesnių bitkoino transakcijų nebus taip patogu ir efektyvu. Lentelės yra didelės, turinčios daug duomenų, todėl užklausa sunaudos daug resursų ir nemokamai suteiktų kreditų gali neužtekti.

Kitas svarstytas variantas yra viešai prieinami bitkoino blokų grandinės duomenys per API prieigą. Tokią paslaugą teikia keletas internetinių tinklalapių. Vienas populiariausių yra *blockchain.com*. Šiame tinklalapyje galime ganėtinai patogiai naviguoti ir analizuoti pavienes transakcijas jų puslapyje. Taip pat jie teikia atvirą API prieigą. Tinklalapio dokumentacijoje yra nurodyti keli skirtingi API bei instrukcijos užklausoms kurti. Išbandytas *Blockchain Data* API pateikia informaciją apie bitkoino bloką, pavienę transakciją, piniginės adresą bei pateikia skirtingus bitkoino bloko analizės grafikus. Šis būdas yra patogus, jeigu norima analizuoti bitkoino bloką. Informacija gaunama apie bloko laiką, aukštį, dydį, bloke esančias transakcijas bei prieš tai buvusio bloko maišą. Šis būdas naudojamas darbe norint gauti visų bloke esančių transakcijų maišas, bloko laiką, dydį. Šiame tinklalapyje pateiktas API, skirtas pavienių transakcijų informacijai, buvo netinkamas todėl, kad užklausos rezultate nėra duomenų apie buvusiosios transakcijos maišą, nors jų API dokumentacijoje teigiama, kad tokia informacija yra teikiama, tačiau išbandžius užklausą praktiškai, transakcijos įvesties maišos reikšmės nebuvo pateikiamos. Tokiu būdu negalime atsekti transakcijų kelio iki senesnių transakcijų, ar netgi iki pirmosios transakcijos kuomet buvo iškastas pradinis bitkoinas. Todėl šis būdas buvo naudojamas tik informacijai apie patį bloką bei bloke esančias transakcijas surinkti.

Kitas tinklalapis *btc.com* siūlo taip pat API prieigą. Šiame tinklalapyje informacija apie transakcijas yra pateikiama išsamesniu būdu bei yra įtraukta buvusiosios transakcijos maiša, įvesčių ir išvesčių dydžiai, įvesties adresai, įvesties buvusiosios transakcijos maiša, įvesties suma, išvesties suma bei išvesties adresą. Kadangi gaunama visa reikalinga informacija, tai šis tinklalapis buvo pasirinktas informacijai apie transakcijas surinkti.

Informacijai per API prieigą pasiekti buvo naudojamas *Python* programavimo kalba bei *Visual Code* programinė įranga. Norint pasiekti transakcijas bei informaciją apie jas, buvo sukurtas algoritmas. Algoritmui yra nurodoma norima bitkoino bloko maiša. Tuomet kreipiamasi į *blockchain.com* API ir gaunama informacija apie patį bloką bei visas bloke patvirtintų transakcijų maišas. Tos transakcijų maišos yra sudedamos į duomenų sąrašą. Tuomet po vieną nurodoma transakcija iš transakcijų maišos duomenų sąrašo bei siunčiama užklausa į *btc.com* API. Gauta transakcijų informacija yra saugoma atskiroje duomenų rinkmenoje. Tuo pačiu prie duomenų sąrašo pridedama įvesties transakcijos maiša (gali būti ir kelios įvesties transakcijos maišos). Tokiu būdu duomenų sąrašas auga apimdamas ne tik pasirinkto bloko transakcijas, bet ir tų transakcijų įvesčių transakcijas bei tų įvesčių transakcijų įvesties transakcijas ir t.t.



4 pav. Bitkoino transakcijų grafo apžvalga

Naudojant šį algoritmą iškilo keletas kliūčių. Visų pirma algoritmo užklausos nutrūkdavo todėl, kad *btc.com* tinklalapis gaudavo per daug užklausų iš vieno kompiuterio bei jos buvo per dažnos. Tokiu būdu tinklalapio ir API kūrėjai nori apsisaugoti nuo per didelio serverių apkrovimo, todėl per dažnas užklausas nutraukia. Siekiant to išvengti algoritmas buvo papildytas funkcija, jeigu negaunamas atsakas dėl užklausos, buvo daroma 5 – 10 sekundžių pauzė ir bandoma siųsti užklausą iš naujo. Tokiu būdu pavyko išvengti algoritmo netikėtų sustojimų. Kita problema buvo ta, kad algoritmas nutrūkdavo, nes senesnėse transakcijos nebūdavo tam tikrų bitkoino transakcijos informacijos laukų, pavyzdžiui, įvesties vertės, nes transakcija yra pati pirmoji. Bitkoino blokų grandinė keitėsi kelis kartus, todėl senesnės transakcijos yra panašios, tačiau gali būti šiek tiek kitokios struktūros. Norint išvengti šios problemos, iš pradžių paleidžiamas algoritmas, kuris surenka visas bloko transakcijas į sąrašą, vėliau iteruojamos kiekviena iš transakcijų ir surenkama informacija apie buvusiąją transakciją. Transakcijos maiša yra prijungiama prie transakcijų maišų sąrašo. Tokiu būdu surenkamas visų bloko transakcijų bei kitų senesnių transakcijų maišų sąrašas. Šis sprendimas padeda todėl, kad turimas galutinis transakcijų sąrašas ir jeigu užklausa nutrūkdavo, galima būdavo patikrinti, kiek transakcijų jau yra išsaugota ir tęsti nuo tos vietos, kur užklausa nutrūko.

Analizės pradžioje norėta parsisiųsti bitkoino transakcijas bei visas buvusiąsias transakcijas, kol jos pasieks naujas iškastas bitkoino monetas. Taigi, norėta turėti visą bitkoino transakcijų istoriją, nuo jų iškasimo blokų grandinėje iki paskutinės transakcijos. Tokiu būdu būtų galima sudaryti visą transakcijos priešistorės medį, kuriame atsiskleistų iš kokių bitkoino monetų sudaryta paskutinė transakcija bei kokia yra tų monetų transakcijų istorija.

Analizuojant tokią galimybę, susidurta su keletu problemų. Visų pirma duomenų kiekis auga ženkliai. Gali būti, kad transakcija yra sudaryta iš kelių, ar kelių dešimčių ar netgi kelių šimtų įvesčių transakcijų, tuo tarpu tos transakcijos gali turėti dar dešimtis įvesčių transakcijų, pastarosios dar kelias dešimtis. Vienos transakcijos gali būti siunčiamos kas kelias dienas ar ilgiau, o kitos transakcijos gali būti siunčiamos kelių minučių skirtumu. Tokiu būdu transakcijų medis išauga nuo kelių šimtų transakcijų iki kelių milijonų transakcijų. Norint išgauti informaciją apie tokį kiekį transakcijų, reikia ieškoti kitų būdų kaip sparčiai bei efektyviai išgauti reikiamą informaciją. Kitas pasiruošimo iššūkis buvo laikas. Algoritmas iš pradžių veikia ganėtinai greitai, todėl kad pirmos

užklausos aptarnaujamos greitai, daugėjant užklausų – atsakymo laikas ilgėja. Šiuo atveju API prieiga nėra pats tinkamiausias būdas, kadangi API serveriai stabdo per dažnas transakcijas, todėl reikia daryti pertraukas tarp užklausų. Trečia problema būtų gautų duomenų apdorojimas. Gautos transakcijos vėliau yra sujungiamos į grafą, todėl sudaryti grafą, kuris turi kelis milijonus viršūnių, užtrunka ilgiau bei vėliau jį analizuoti bus sunkiau, nes visos užklausos bus apdorojamos daug ilgesnį laiką. Esant tokiam dideliam duomenų kiekiui *Python* programavimo kalba nėra efektyvi bei tokiu atveju patartina naudoti *Spark* programavimo kalbą. Ketvirta, pavaizduoti tokio dydžio grafą yra praktiškai neįmanoma, kadangi visos viršūnės persidengia bei persipina tarpusavyje. Penkta, net greitai veikiantis algoritmas užtruks daugiau nei savaitę norint tiesiog parsiųsti duomenis lokaliai.

Kadangi transakcijų kiekis yra labai didelis, todėl nuspręsta apriboti naujesnio bloko transakcijų skaičių iki 10 žingsnių atgal. Vadinasi, naujesnio bloko transakcijų grafai bus sudaryti iš galutinės transakcijos bei 10 transakcijų iki tol. Šis sprendimas priimtas todėl, kad, norint analizuoti naujausius bitkoino transakcijų duomenis, transakcijų skaičius auga labai ženkliai bei turimi kompiuteriniai resursai nebepajėgia efektyviai susitvarkyti su turima informacija bei jos kiekiu. Todėl šios analizės metu bus naudojamas mažesnis duomenų rinkinys, siekiant sudaryti modelio prototipą, kurį galima būtų panaudoti ir didesniam bitkoino transakcijų medžiui, turint atitinkamus resursus.

Galiausiai buvo naudojami skirtingi duomenų išgavimo būdai. Keli skirtingi būdai buvo apjungti, kad gauti reikiamą duomenų rinkinį greitai ir efektyviai. Visų pirma bloko transakcijų maišos buvo gautos naudojant *blockchain.com* tinklalapio siūlomą API prieigą. Toliau šios transakcijos buvo naudojamos *btc.com* API prieigoje, siekiant pasiekti buvusiosios transakcijos maišą. Transakcijos maišos bei buvusiosios transakcijos maišos duomenų poros buvo išsaugomos atskirame duomenų rinkinyje. Toliau naudojamas algoritmas surenka informaciją apie transakcijas. Kadangi po tam tikro laiko IP adresas buvo užblokuotas, tai likusios transakcijos buvo pasiektos naudojant „*Google Big query*“. Informacijos išgavimas naudojant SQL užklausą yra daug kartų lėtesnis nei naudojant API prieigą, tačiau „*Google Big query*“ buvo pasirinktas todėl, kad likusių neišgautų transakcijų skaičius nebuvo didelis.

2.2. Duomenų rinkinio pasiruošimas

Tyrime naudojama tik dalis transakcijų informacijos. Buvo pasirinkti tik tam tikri duomenys, kurie yra aktualūs šioje analizėje. Kadangi siekiama pateikti paskutinių transakcijų priešistorę bei įvardinti iš kokių bitkoino monetų yra sudaryta galutinė transakcija bei kokia tų monetų istorija, todėl pasirinkti tik tam tikri informacijos laukai. Duomenų laukai buvo apriboti ir dėl spartesnio algoritmo veikimo. Galutinis duomenų rinkinys apie transakcijas turi tokią informaciją:

3 lentelė. Transakcijų informacijos pasirinkti laukai tyrimui

Lauko pavadinimas	Lauko paaiškinimas	Lauko dydis
Bloko maiša	Bitkoino bloko identifikacinė vertė.	Tekstas
Bloko sukūrimo laikas	Laikas, kuris parodo, kada buvo sugeneruotas blokas.	Data
Įvesčių skaičius	Nurodo transakcijos įvesčių skaičių.	Skaičius

Išvesčių skaičius	Nurodo transakcijos išvesčių skaičių.	Skaičius
Mokestis	Nurodo transakcijos mokestį.	Skaičius
Ar pradinė transakcija	Identifikuoja ar transakcija yra pirmoji (naujai iškastas bitkoinas).	Tiesa / Netiesa
Įvesties transakcijos maiša	Nurodo prieš tai buvusios transakcijos identifikaciją.	Tekstas
Įvesties vertė	Nurodo siunčiamų bitkoinų dydį iš įvesties piniginės.	Skaičius
Išvesties vertė	Nurodo, kiek bitkoinų siunčiama į išvesties piniginę.	Skaičius

Analizė buvo pradėta tiriant 100 000 bloką. Šis blokas yra iškastas 2010 metų gruodžio 29 dieną. Jį sudaro tik 4 transakcijos. Tuo metu bitkoinas dar nebuvo toks populiarus, todėl transakcijų skaičius bloke buvo ženkliai mažesnis. Taigi šios 4 transakcijos, naudojant algoritmą, buvo atsekamos iki pradinės transakcijos, kai bitkoino moneta buvo iškasta. Galutinį transakcijų maišos sąrašą sudarė tik 97 transakcijos bei buvo sudaryti 4 transakcijų medžiai, kurie siekė iki pirmųjų iškastų bitkoino monetų. Įvykdyti šį algoritmą prireikė tik 3 minučių. Matome, kad 100 000 bloke, gavus istorines transakcijas, transakcijų sąrašas padidėjo daugiau nei 24 kartus.

Kitas blokas 200 000 buvo iškastas po poros metų nuo 100 000 bloko, 2012 metų rugsėjo 22 dieną. Šį bloką sudaro jau 388 transakcijos. Matome, kad transakcijų skaičius didėjo ženkliai, tačiau bitkoinas vis dar nebuvo toks populiarus, koks yra dabar. Taigi, pritaikius duomenų išgavimo algoritmą, kartu su pradinėmis transakcijomis transakcijų maišos sąrašas padidėjo iki 12 029. Algoritmas užtruko 6,5 valandos, kol surinko reikiamą informaciją apie transakcijas bei jų istoriją. Šiuo atveju transakcijų sąrašas padidėjo 31 kartą.

Naujesnis blokas 700 000, kuris buvo iškastas 2021 metų rugsėjo 11 dieną, turi 1 276 transakcijas. Kadangi šis blokas yra ganėtinai naujas, šiame bloke gali būti transakcijų, kurios turi tik kelias arba dešimtis transakcijų iki pradinės transakcijos, tačiau gali būti transakcijų, kurių metu yra naudojamos bitkoino monetos, kurios buvo iškastos 2015 metais ar seniau, todėl transakcijų skaičius gali būti ženkliai didesnis nei lyginant su senesniais blokais. Šių transakcijų gavimui buvo naudojamas tas pats algoritmas. Algoritmas apskaičiavo, kad kartu su pradinėmis transakcijomis viso bus 738 592 transakcijos, tačiau pradėjus nuosekliai tikrinti duomenų rinkinį pastebėta, kad tai nėra visos transakcijos. Taip nutiko todėl, kad užklausų buvo per daug ir buvo pasiektas maksimalus užklausų kiekis bei serveris užblokavo kompiuterio IP adresą, todėl algoritmas nutrūko bei neberinko informacijos. Esant tokiai situacijai buvo nuspręsta apriboti transakcijų istoriją iki 10 žingsnių atgal. Surinktos transakcijos buvo naudojamos sudarant 10 žingsnių transakcijų medžius. Dauguma transakcijų jau turėjo 10 žingsnių informaciją. Transakcijų medžiai, kurios neturėjo visų 10 žingsnių transakcijų informacijos, buvo papildomi naudojant „*Google Big query*“. Šis procesas užtruko ilgiau nei buvo renkama informacija per API prieigą, apie 20 valandų. Kad išgauti visą reikiamą 10 žingsnių informaciją 700 000 bloko transakcijoms, prireikė daugiau nei savaitės.

Toliau analizėje sudaromas kiekvienos transakcijos grafas. Duomenų lentelė yra papildoma informacija susijusia su grafų savybėmis – viršūnių skaičius, briaunų skaičius, aukščiausias grafo viršūnės laipsnis, vidutinis grafo viršūnės laipsnis. Galutinis duomenų rinkinys turi informaciją apie transakcijas bei transakcijų grafo savybes.

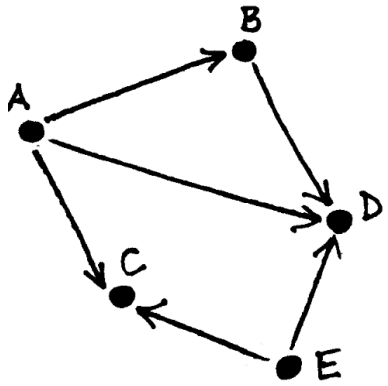
2.3. Grafų panaudojimas transakcijų medžio sudaryme

Grafų teorija – matematikos mokslo šaka, kuri atsirado XVIII amžiuje bei tiria savybes grafų, kuriuos sudaro viršūnės ir jas jungia briaunos.

Grafu G yra vadinama viršūnių ir briaunų aibių pora (V, E) ir žymima

$$G = (V, E).$$

Jei grafo briaunos turi kryptis, tai tuomet grafas vadinamas orientuotu grafu [65].



5 pav. Orientuotas grafas [65]

Grafo viršūnės laipsnis yra lygus lankų, kurie išeina arba įeina iš šios viršūnės, skaičiui.

Medžiu vadinamas grafas, kuris neturi ciklų [65].

Šiame tyrime grafo viršūnės yra transakcijos, o grafo briaunos atitinka transakcijos įvestį t.y. buvusiąją transakciją. Kryptis nustatoma iš seniausios transakcijos į naujausią transakciją, vadinasi, grafuose visos kryptys veda į viršūnę, kuri atitinka 700 000 bitkoino bloko transakciją.

2.4. Duomenų rinkinio požymiai naudojami klasterizavime

Tiriant bitkoino transakcijas, vienas iš svarbiausių požymių yra laikas. Daugelyje tyrimų yra naudojamas transakcijos atlikimo laikas arba laiko skirtumas tarp transakcijų. Ruošiant galutinį duomenų rinkinį, kuris bus naudojamas klasterizavimo metoduose, buvo išskirti šie požymiai:

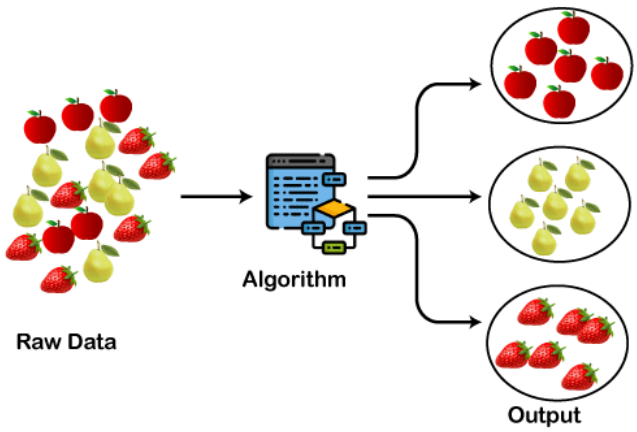
- Grafo viršūnių skaičius. Apskaičiuojamas sudarant transakcijų grafą. Šis skaičius taip pat parodo transakcijų skaičių transakcijų grafe.
- Grafo briaunų skaičius. Apskaičiuojamas sudarant transakcijų grafą. Šis skaičius parodo transakcijų grafe esančių įvesčių skaičių.
- Aukščiausias grafo viršūnės laipsnis. Įvertis parodo, kiek daugiausiai įvesčių buvo vienoje iš transakcijų.

- Vidutinis grafo viršūnės laipsnis. Įvertis parodo, kiek vidutiniškai įvesčių buvo transakcijose.
- Transakcijos mokesčio vidurkis.
- Vidutinis įvesčių skaičius transakcijoje.
- Vidutinis išvesčių skaičius transakcijoje.
- Vidutinė įvesties suma. Šis skaičius yra paverčiamas iš satošių į bitkoinus.
- Didžiausia įvesties suma. Šis skaičius yra paverčiamas iš satošių į bitkoinus.
- Mažiausia įvesties suma. Šis skaičius yra paverčiamas iš satošių į bitkoinus.
- Vidutinis transakcijų laiko skirtumas minutėmis. Šis įvertis randamas apskaičiuojant skirtumą tarp transakcijų laiko bei tuomet paskaičiuojamas vidurkis. Šis skaičius išreiškiamas minutėmis.
- Transakcijos laiko skirtumo minutėmis standartinis nuokrypis.
- Įvesčių skaičiaus standartinis nuokrypis.
- Išvesčių skaičiaus standartinis nuokrypis.
- Įvesties sumos standartinis nuokrypis.
- Transakcijos mokesčio standartinis nuokrypis.
- Laiko skirtumas tarp seniausios ir naujausios transakcijos minutėmis. Šis skaičius parodo laiko skirtumą tarp pirmosios ir paskutinės transakcijos minutėmis.
- Didžiausias transakcijų skaičius per dieną. Šis skaičius parodo kiek daugiausia transakcijų buvo atlikta per dieną.
- Ilgiausias laiko skirtumas tarp transakcijų minutėmis. Šis skaičius parodo didžiausią laiko skirtumą transakcijų minutėmis.
- Trumpiausias laiko skirtumas tarp transakcijų minutėmis. Šis skaičius parodo mažiausią laiko skirtumą tarp transakcijų minutėmis.

Šis duomenų rinkinys yra naudojamas klasterizavimo metoduose.

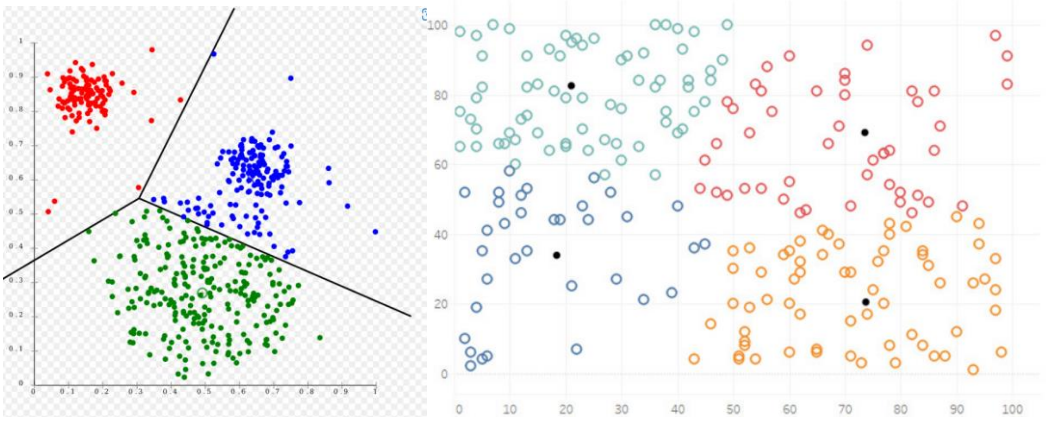
2.5. Klasterizavimo metodai

Klasterinė analizė – tai duomenų analizės metodas, kurio metu identifikuojamos homogeninės stebėjimų grupės. Kiekvienoje grupėje yra priskirti objektai, kurie kiek galima daugiau yra panašūs į kitus grupėje esančius metodus. Šis analizės metodas yra priskiriamas mašininiam mokymuisi be mokytojo, todėl duomenų grupės, taip vadinami klasteriai, nėra iš anksto nuspręsti [61].



6 pav. Klasterizavimo metodų esmė [62]

Objektų panašumas tarpusavyje yra matuojamas atstumu. Paprasčiausiai galima nustatyti objektų klasterius nubrėžiant duomenų taškų sklaidos diagramą. Jeigu duomenų nėra daug bei jie turi aiškias skirtingas grupes, tuomet ganėtinai lengva nustatyti skirtingus klasterius vien pažiūrėjus į grafiką. Tačiau kai duomenų kiekis didėja, labai retai galima atskirti skirtingas grupes grafiškai. Tokiu atveju neretai skirtingi taškai persidengia bei klasteriai nėra aiškiai atskirti vienas nuo kito.



7 pav. Klasterizavimo pavyzdžiai [63, 64]

Dažniausiai klasterizavimo metodai naudojami norint sugrupuoti duomenis į tam tikras grupes pagal panašumą arba norint paruošti duomenis kitiems mašininio mokymo metodams. Pirmuoju atveju sugrupuoti duomenys naudojami [61]:

- marketingo srityje, kuomet siekiama išskirstyti vartotojus į skirtingas grupes, tuomet galima komunikuoti reklaminę žinutę pagal atitinkama vartotojų segmentą;
- rizikos analizėje, kuomet siekiama identifikuoti įtartinus finansinius veiksmus, skirstant vartotojus pagal banko sąskaitos balansą ar atliekamus panašius finansinius veiksmus;
- nekilnojamo turto analizėje, kuomet nekilnojamas turtas yra skirstomas į atitinkamas grupes pagal namo dydį, lokaciją, kainą bei kitas savybes.

Antruoju atveju klasterizavimo metodai naudojami siekiant parodyti duomenų rinkinio išskirtis ar akivaizdžias grupes, kurios vėliau gali būti pašalinamos iš duomenų rinkinio. Tuomet mašininis mokymasis duomenų klasifikacijai yra paprastesnis.

Tyrime pritaikyti skirtingi klasterizavimo metodai siekiant palyginti gautus rezultatus bei atrasti tinkamiausią metodą. Klasterizavimo metodai yra skirstomi į hierarchinius bei nehierarchinius metodus.

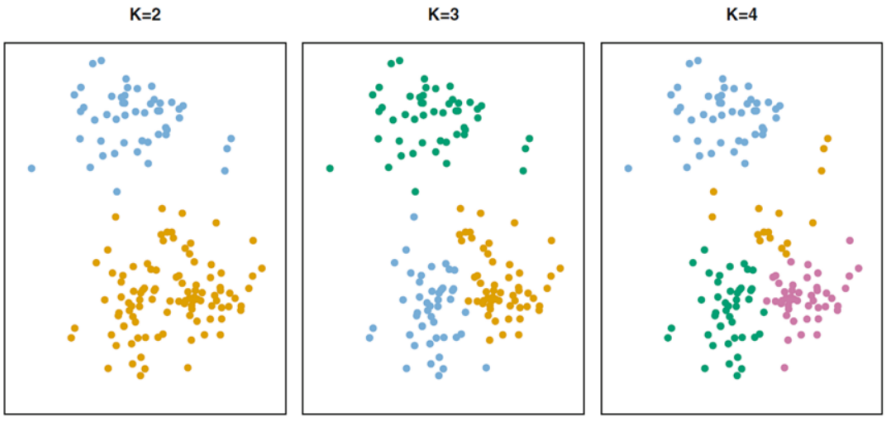
2.6. K-vidurkių klasterizavimo metodas

K-vidurkių metodas priskiriamas nehierarchiniam klasterizavimui. Nehierarchinis klasterizavimas yra taikomas tuomet, kuomet yra žinomas klasterių skaičius arba klasterių skaičius yra lengvai pasirenkamas. Tokiu atveju metodas žino, kiek klasterių turi būti bei bando priskirti duomenis skirtingiems klasteriams. Vienas iš populiariausių tokių metodų yra k-vidurkių metodas [66].

K-vidurkių metodo esmė yra:

1. suskirstyti duomenis į *k* pradinių klasterių,
2. apskaičiuoti kiekvieno duomenų objekto atstumą iki *k* klasterio centro,

3. priskirti objektą duomenų klasteriui *k*,
4. perskaičiuoti duomenų klasterio *k* centrus,
5. perskirstyti objektus į *k* klasterius,
6. vykdyti algoritmą, kol nebereikia objektų perskirstyti.

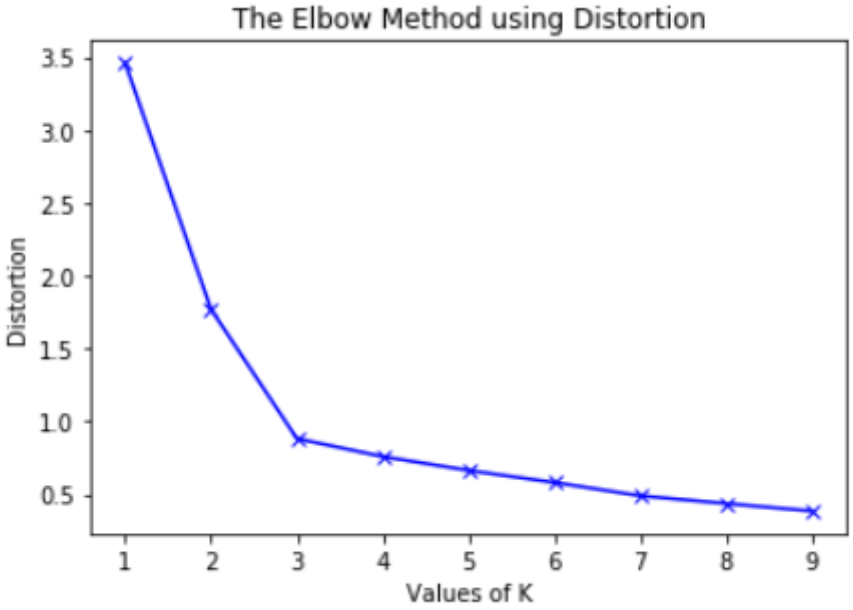


8 pav. K-vidurkių metodo eiga [67]

Metodo idėja yra sudaryti tokias objektų grupes, kurios turi kuo mažesnius skirtumus tarpusavyje. Objektai k-vidurkių metode priskiriami klasteriams apskaičiuojant atstumą. Yra skirtingų būdų, kaip apskaičiuoti atstumą, tačiau vienas iš populiariausių yra Euklido atstumo kvadratas. Euklido atstumo kvadratas yra apskaičiuojamas [67]:

$$d(X,Y) = \|X - Y\| = \sum_{i=ą}^{m} (x_i - y_i)^2.$$

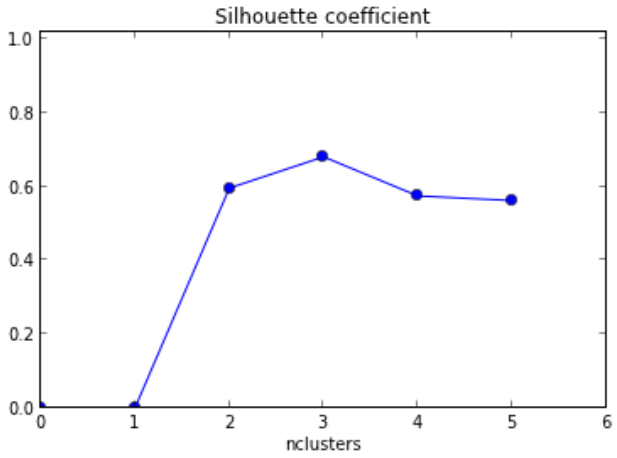
Kadangi šiame metode klasterių skaičius yra laisvai pasirenkamas, todėl galima pritaikyti skirtingus metodus, kad parinkti tinkamą klasterių skaičių. Pagrindiniai yra alkūnės (angl. *Elbow*)bei *Silhouette* metodai.



9 pav. Alkūnės metodas naudojamas parinkti klasterių skaičiui [68]

Paveikslėlyje yra vaizduojamas alkūnės metodo rezultatas. Rekomenduojamas klasterių skaičius yra pasirenkamas, kai kreivė yra „alkūnės“ lygyje, tai šiuo atveju yra siūlomi 3 klasteriai. Vėliau po 3 klasterio nėra tokio didelio skirtumo tarp kitų klasterių, todėl 3 yra optimalus variantas [68].

Kitas metodas yra *Silhouette* koeficiento apskaičiavimas. Šis koeficientas palygina vidutinius atstumus tarp objektų klasteriuose su vidutiniais atstumais tarp kitų klasterių. Jeigu *Silhouette* koeficientas yra didelis, tai objektai laikomi klasterio nariais, o jeigu koeficientas yra mažas – išskirtimis. Labai dažnai šis koeficientas yra naudojamas kartu su k-vidurkių metodu [70].



10 pav. *Silhouette* koeficiento vaizdavimas grafike [69]

K-vidurkių metodo privalumai [67] yra, kad šį metodą galima taikyti pažingsniui ir matyti, kaip keičiasi klasteriams priskirti objektai. Taip pat metodas naudoja aiškiai apibrėžtą algoritmą, kurį galima pritaikyti bet kokioje programavimo kalboje. K-vidurkių metodo trūkumai yra tai, kad

algoritmas ilgai skaičiuoja rezultatą, todėl naudojant ganėtinai didelį duomenų rinkinį, algoritmas užtruks ilgą laiko tarpą.

2.7. Hierarchiniai klasterizavimo metodai

Hierarchiniai klasterizavimo metodai yra skirstomi į dvi grupes: jungimo algoritmai (angl. *agglomerative*) ir skaidantys (angl. *divisive*) algoritmai. Jungimo klasterizavimo metodas vykdomas taip, kad iš pradžių objektai yra laikomi vienu dideliu klasteriu. Toliau objektai yra skaidomi į grupes bei taip susidaro nauji klasteriai. Skaidymo klasterizavimo metodas yra atvirkščias jungimo metodams, iš pradžių objektai yra paskirstyti į mažus klasterius bei yra jungiami sudarant vis didesnius klasterius [66].

Jungimo algoritmas yra vykdomas taip:

1. Yra *N* klasterių, kurie turi po vieną objektą bei yra atstumų simetrinė matrica, kurios dydis *NxN*.
2. Tuomet yra nustatomi du klasteriai, kurie yra panašiausi, vadinasi, tarp jų atstumas yra mažiausias.
3. Tuomet klasteriai yra sujungiami.
4. Vėlgi ieškomi du klasteriai, kurių atstumas yra panašiausias.
5. Šie klasteriai yra sujungiami.
6. Kartojami tie patys žingsniai, kol lieka vienas klasteris.

Skaidymo metodas vyksta atvirkščiai.

Naudojant jungimo algoritmus, reikia pasirinkti, kokiu būdu klasteriai bus apjungti. Galima jungti klasterius naudojant tolimiausio ar artimiausio kaimyno panašumo matą, centrų panašumo matą ar vidutinės jungties.

Artimiausio kaimyno panašumo matas apskaičiuojamas:

$$d(U,V) = \min_{X_i \in U, Y_i \in V} d(X_i, Y_i).$$

Tolimiausio kaimyno panašumo matas apskaičiuojamas:

$$d(U,V) = \max_{X_i \in U, Y_i \in V} d(X_i, Y_i).$$

Vidutinės jungties panašumo matas apskaičiuojamas:

$$d(U,V) = \sum_{X_i \in U} \sum_{Y_i \in V} \frac{d(X_i, Y_j)}{n_U n_V},$$

kur n_U – klasterio *U* objektų skaičius, n_V - klasterio *V* objektų skaičius.

Centrų panašumo matas apskaičiuojamas:

$$d(U,V) = d(\bar{U}, \bar{V}).$$

2.8. Tankiu grįsti klasterizavimo metodai

Tankiu grįsti klasterizavimo metodai suskirsto objektus į klasterius pagal tai kaip objektai yra išsidėstę, ten kur objektai pasiskirstę tankiau, tuomet objektai priskiriami tam pačiam klasteriui. Jeigu yra objektų, kurie išsidėstę tarp klasterių, tuomet jie yra laikomi triukšmu.

Populiariausias tankiu grįstas metodas yra DBSCAN (angl. *density-based spatial clustering of applications with noise*). DBSCAN metode reikia nurodyti du parametrus: epsilon, kuris nurodo minimalų reikalaujamą atstumą tarp klasterio objektų, kad klasterio objektai būtų laikomi to pačio klasterio nariais, ir minimalų taškų skaičių, kuris parodo, koks yra minimalus objektų skaičius, kad būtų galima sudaryti klasterį.

Šio metodo veikimo algoritmas [71]:

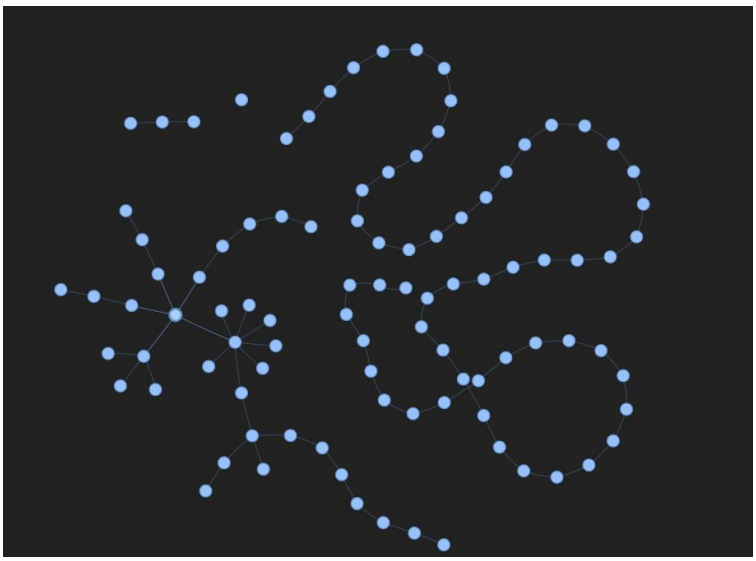
1. Pasirenkamas objektas iš duomenų rinkinio bei ieškomi visi artimiausi kaimynai pagal pasirinktą epsilon reikšmę.
2. Jeigu rastų objektų skaičius yra didesnis nei pasirinktas minimalus objektų skaičius, tuomet objektai yra priskiriami klasteriui.
3. Kitiems objektams, kurie dar nėra priskirti prie klasterių, sukuriamas naujas klasteris.
4. Skaičiuojami atstumai bei priskiriami kiti objektai prie klasterio.
5. Tokiu būdu skaičiuojami objektų atstumai ir jie paskirstomi po klasterius. Jeigu objektas netinka nei vienam iš klasterių, tuomet jis yra pripažįstamas triukšmu.

Sunkiausia šiame klasterizavimo metode yra nustatyti tinkamus epsilon bei mažiausią objektų skaičių. Jeigu parametrų įverčiai pakeičiami net ir neženkliai, metodo rezultatai gali labai skirtis.

2.9. Grafų vaizdavimas su *Python* biblioteka *pyvis*

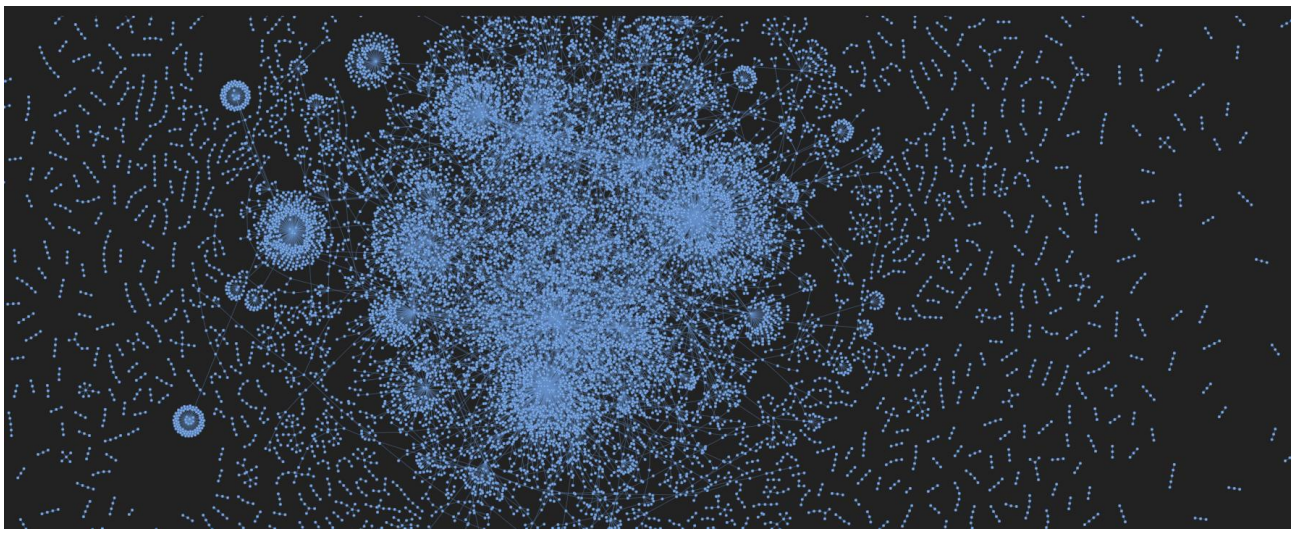
Turint galutinį duomenų rinkinį lentelėje yra ganėtinai sudėtinga matyti visą transakcijų medį. Transakcijų medžiui pavaizduoti geriausiai tinka grafai. Kadangi duomenų rinkinio sudaryme naudojama *Python* programavimo kalba, todėl iš pradžių pasirinkta viena iš *Python* bibliotekų *pyvis*, kuri tinkama grafų vaizdavimui. Taip pat ši biblioteka sugeneruoja *html* duomenų failą, kuriame galima interaktyviai analizuoti transakcijas, judinti grafo viršūnes, tempti į šalis, matyti grafo viršūnių reikšmes, jeigu jos yra priskirtos.

Paveikslėlyje (**11 pav.**) pavaizduotas bitkoino 100 000 bloko visų transakcijų grafai. Kaip ir minėta anksčiau, šis blokas turi 4 transakcijas. Matome paveikslėlyje 4 atskirus grafus: pirmąjį sudaro viena transakcija, antrąjį sudaro 3 transakcijos, trečiąjį sudaro viena ilga transakcijų eilė, o ketvirtasis grafas yra sudarytas iš skirtingų įvesčių skaičiaus. Tokiu būdu galime pavaizduoti visas bloko transakcijas viename grafike.



11 pav. Bloko 100 000 transakcijų grafai

Bitkoino 200 000 bloką sudaro 388 transakcijos, taigi visas transakcijas pavaizduoti viename grafike yra sudėtinga. Paveikslėlyje (12 pav.) matome, kad naudojant tą pačią *pyvis* biblioteką, atsekti, kur prasideda ar baigiasi viena ar kita transakcija, nėra lengva. Matome, kad yra daug pavienių transakcijų grafų, kurie sudaryti tik iš 1-3 transakcijų, tačiau yra daug įdomios sandaros grafų, kuriuos įvertinti viename grafike yra sudėtinga. Taip pat toks grafiko sukūrimas, kuriame būtų pavaizduoti visi vieno bloko transakcijų medžiai, reikalauja daugiau resursų bei daugiau laiko. Šio grafiko sukūrimas užtruko pora valandų. Kadangi šis bitkoino blokas yra ganėtinai senas bei transakcijų nebuvo daug, o ir transakcijų medžiai nėra tokie ilgi, kaip šių dienų bitkoino blokuose, todėl ši biblioteka nėra tinkama vaizduoti visiems transakcijų grafams viename grafike.

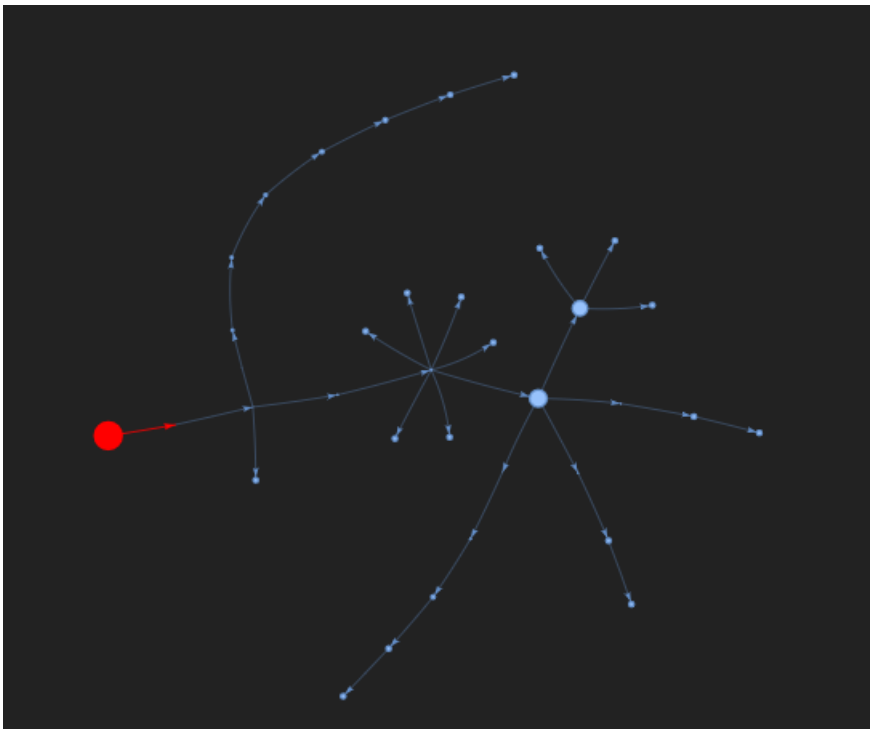


12 pav. Bloko 200 000 transakcijų grafai

Norint pavaizduoti visus bloko transakcijų grafus viename grafike, buvo išbandyta *Python* biblioteka *Networkx* bei *Gephi* programinė įranga. *Networkx* biblioteka nėra tinkama dideliems grafų vaizdavimams. Ji nesukuria interaktyvių grafų, kaip *pyvis* biblioteka, todėl grafai yra pavaizduojami greičiau, tačiau jie persidengia vienas per kitą ir nėra lengva suprasti bei atskirti skirtingus grafus. *Gephi* programinė įranga yra sukurta specialiai didelių grafų vaizdavimams.

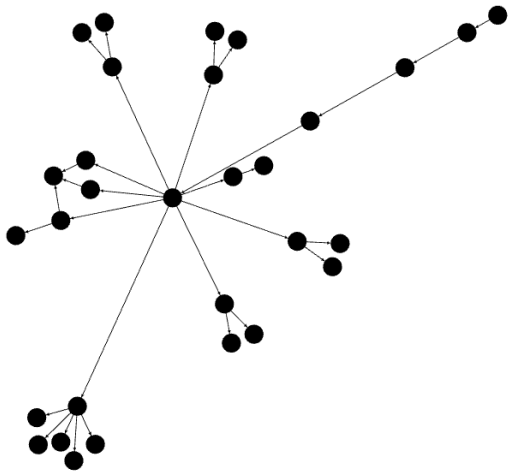
Tačiau kadangi 700 000 blokas turi 1 276 transakcijas, pavaizduoti visas jas viename grafike nėra tikslinga. Transakcijų medžiai yra per dideli bei nebus lengva atskirti skirtingus transakcijų grafus.

Analizėje vaizduosime po vieną grafą atskirai, kad aiškiau matytųsi grafo struktūra. Naudojant *pyvis* biblioteką, galima nupiešti gražų grafą, kuriame matosi transakcijų kryptis bei kiekviena grafo viršūnė turi atitinkamą dydį, kuris priklauso nuo įvesties sumos.



13 pav. Bloko 100 000 vienos iš transakcijų grafo vaizdavimas su *pyvis* biblioteka

Gephi programinėje įrangoje taip pat galima nustatyti kryptį. *Gephi* daugiau tinka didelės apimties grafams vaizduoti bei grafų apdorojimas vyksta greičiau. Ši programa patogi tuo, kad turi vartotojui draugišką aplinką, kurioje galima bandyti keisti parametrus bei bandyti aiškiai pavaizduoti didelį grafą. Tiesa, jeigu grafai yra ypač dideli bei turi didelį skaičių įvesčių, pavaizduoti juos aiškiai ir suprantamai nėra paprasta.



14 pav. Grafo vaizdavimas naudojantis *Gephi* programa

2.10. Naudojama programinė įranga

Šiame darbe duomenų apdorojimui yra naudojami kelios skirtingos programinės įrangos.

- *Python* programavimo kalba.
- Duomenys yra pasiekiami per API prieigą, naudojant *Python* programavimo kalbą.
- „*Google Big Query*“ yra duomenų rinkinys „*Bitcoin*“. Jis naudojamas likusių transakcijų informacijai surinkti.
- R programinė įranga naudojama duomenų apžvalgomajai analizei.

Sudarant galutinį duomenų rinkinį yra naudojamos *Python* bibliotekos:

- *Pandas* biblioteka yra naudojama duomenų analizei ir duomenų apdorojimui.
- *Google.cloud* biblioteka yra naudojama prisijungti prie *„Google cloud“*.
- *Networkx* biblioteka naudojama sudarant transakcijų grafą.
- *Pyvis* biblioteka naudojama grafų pavaizdavimui, kuomet transakcijų grafas yra ne per didelis.
- *SKLearn* biblioteka yra naudojama duomenų klasterizavime.
- *Matplotlib* biblioteka yra naudojama grafikų vaizdavime.

3. Tyrimų rezultatai ir jų aptarimas

3.1. Duomenų rinkinio apžvalga bei aprašomoji analizė

Analizėje yra tiriamas 700 000 bitkoino blokas bei transakcijos jame. Visų pirma algoritmai buvo išbandyti 100 000 bei 200 000 blokams, siekiant optimizuoti algoritmą bei pritaikyti jį didesniam duomenų kiekiui. Taip pat šie senesni blokai neturi tiek daug transakcijų bei jų transakcijų medžiai nėra dideli. 700 000 bitkoino blokas pasirinktas dėl apvalaus bloko numerio. Šis blokas yra iškastas 2021 metų rugsėjo 11 dieną, jis yra ypatingas tuo, kad bloko iškasimo dieną jau buvo 89,58% bitkoino monetų cirkuliacijoje. Bitkoino rinkos kaina tuo metu siekė 45 201 JAV dolerių [72]. Tai yra ganėtinai didelė bitkoino kaina bei tai parodo, kad bitkoinas buvo labai populiarus tuo metu ir plačiai perkamas. Tuo metu rinka buvo aukštumose, taip vadinama bulių rinka (angl. *bull market*), kurios metu pirkėjai labai pasitiki rinka, perka monetas, investuoja, tikėdamiesi didelės grąžos. Dažniausiai tokiu laikotarpiu yra maža pasiūla ir didelė paklausa, todėl kainos yra ženkliai pakilusios, rinka vadinama perpirkta (angl. *overbought market*) [74].

Šiame bloke yra 1 276 transakcijos. Pati pirmoji transakcija visada yra bloko iškasimo apdovanojimo transakcija, todėl grafai yra sudaryti 1 275 transakcijoms. Pirmojoje transakcijoje yra iškastos naujos bitkoino monetos, todėl ši transakcija neturi istorijos. Šio bloko pirmoji transakcija skiria kasėjams apdovanojimą vertą 6,25 bitkoino.

4 lentelė. Duomenų rinkinio žvalgomoji analizė

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	1275	639	368	2	320	958	1276
Number_of_nodes	1275	32381	85291	5	11	4610	583767
Number_of_edges	1275	46529	128241	4	10	4864	910862
Highest_graph_degree	1275	226	349	2	2	476	1038
Average_graph_degree	1275	2.1	0.49	1.6	1.8	2.1	5.6
Fee_average_btc	1275	0.0014	0.0043	0.00000035	0.000036	0.0021	0.12
Average_input_counts	1275	76	115	0.75	1	156	565
Average_output_counts	1275	33	56	1.1	2.9	41	1113
Average_input_value_btc	1275	22	102	0.00028	1	8.4	2803
Max_input_value_btc	1275	7482	14514	0.0003	4.5	3000	45493
Min_input_value_btc	1275	1.1	7.5	0.00000001	0.0000055	0.018	194
Average_transaction_time_diff_min	1275	12818	55202	0	209	3341	697907
Block_time_std	1275	61195	152997	0	833	62267	1544979
Input_count_std	1275	65	95	0	0	160	358
Output_count_std	1275	88	209	0	1.3	123	6195
Value_std	1275	79	175	0.0000085	0.76	100	2989
Fee_std	1275	0.0028	0.0083	0	0.000019	0.0028	0.19
Difference_newest_oldest_transaction_dates_in_min	1275	514658	922031	0	1135	524226	4337221
Max_number_of_tran_per_day	1275	1680	4272	1	5	268	29205
Max_time_min	1275	501156	907650	0	1244	483071	4337223
Min_time_min	1275	117	1524	0	1.9	20	50277

Aukščiau pateiktoje lentelėje (žr. 4 lentelėje) yra bendra galutinio duomenų rinkinio aprašomoji statistika. Šiame duomenų rinkinyje yra pateiktos bitkoino transakcijų reikšmės bei bitkoino

transakcijų grafų savybės. Matome, kad viršūnių skaičius (lentelėje *Number_of_nodes*) yra ganėtinai skirtingas. Mažiausia reikšmė yra tik 5 viršūnės, o didžiausia net 583 767 viršūnės. Tai parodo, kad šiame duomenų rinkinyje yra tiek naujesnės bitkoino monetos, kurios turi tik kelias įvykusias transakcijas, tiek ganėtinai senos bitkoino monetos su didesne istorija. Vidutiniškai grafas turi 32 381 viršūnes. Didžiausias grafo viršūnių laipsnis (lentelėje *Highest_graph_degree*) parodo, kiek daugiausiai grafo viršūnė turi briaunų. Šiuo atveju maksimalus skaičius yra 1 038, taigi, viename iš grafų yra transakcija, kurios įvesties transakcijų skaičius siekė net 1 038. Vadinasi, ši transakcija buvo sudaryta iš labai didelio skaičiaus skirtingų transakcijų. Tuo tarpu vidutinis grafo viršūnės laipsnis (lentelėje *Average_graph_degree*) siekia tik apie 2,1. Jeigu pažiūrėsime į didžiausią įvesties sumą (lentelėje *Max_input_value_btc*) bei mažiausią įvesties sumą (lentelėje *Min_input_value_btc*) matysime, kad daugumoje transakcijų vyrauja mažos bitkoino sumos. Paskutiniame kvartilyje matome, kad didžiausia suma svyruoja nuo 3 000 iki net 45 493 bitkoinų. Taip pat įdomu, kad daugumoje, trijuose kvartiliuose visų duomenų, yra įvykdomos iki 268 transakcijų per dieną (lentelėje *Max_number_of_tran_per_day*).

Transakcijų laikas yra labai įvairus. Vieni vartotojai, kurie nevykdo jokios įdomesnės veiklos, vykdo bitkoino transakcijas pakankamai lėtai. Vidutinis maksimalus laikas tarp transakcijų (lentelėje *Max_time_min*) siekia net 501 156 minutes, tai maždaug 348 dienos. Tokių transakcijų savininkai tikriausiai turi bitkoiną daugiau kaip ilgalaikę investiciją bei nedaro didelių pakitimų savo investicijų portfelyje. Kitas rodiklis, vidutinis minimalus laikas tarp transakcijų, (lentelėje *Min_time_min*) siekia 117 minučių, tai transakcijos, dažniausiai vykdomos ne greičiau nei kas 2 valandas. Minimalus laikas tarp transakcijų lygus 0. Taip gali nutikti dėl kelių priežasčių. Visų pirma, bitkoino blokų laikai nėra visiškai tikslūs. Bitkoino bloko laikas gali svyruoti netgi apie 2 valandas. Bitkoino bloko laikas patvirtinamas tuomet, kai jo mediana yra didesnė nei buvusių 11 blokų [74]. Todėl gali pasitaikyti blokų su tuo pačiu laiku. Antra, taip gali nutikti todėl, kad dar nepatvirtinta transakcija naudojama kitoje transakcijoje. Tokiu atveju antroji transakcija turi didesnį transakcijos patvirtinimo mokestį, tačiau norint patvirtinti šią transakciją, reikia pirmiau patvirtinti buvusiąją transakciją. Tokiu būdu abi transakcijos (ar daugiau) atsiduria viename bloke, nes kasėjai siekia gauti didesnį apdovanojimą ir renkasi patvirtinti kelias transakcijas dėl didesnio transakcijų mokesčio [75]. Tokios transakcijos yra įdomesnės, nes įdomios priežastys, kodėl siekiama įvykdyti kelias transakcijas kuo greičiau. Skirtumo tarp naujausios ir seniausios transakcijų rodiklio (lentelėje *Difference_newest_oldest_transaction_dates_in_min*) mažiausią vertė yra 0. Vadinasi, šiame bloke yra bent vienas transakcijų grafas, kurio visos 10 žingsnių transakcijos yra patvirtintos tame pačiame bloke. Kitas įdomus rodiklis yra transakcijų per dieną skaičius (lentelėje *Max_number_of_tran_per_day*). Šis rodiklis parodo, kiek transakcijų iš transakcijų grafo yra atliktos tą pačią dieną. Matome, kad trijuose kvartiliuose visų duomenų yra atlikta mažiau nei 268 transakcijos per dieną. Paskutiniame kvartilyje yra transakcijų kurios siekia kelis tūkstančius transakcijų per dieną. Taip pat matome, kad vidurkio reikšmė yra ganėtinai didelė ir lygi 1 680 transakcijų per dieną. Galima įtarti, kad šiame bloke yra transakcijų grafų, kurių metu transakcijos vykdomos ypatingai greitai.

Duomenų rinkinio aprašomoji analizė rodo, kad rinkinyje vyrauja tipiškos pavienės negreitos bei nedidelių sumų transakcijos. Tačiau rinkinyje taip pat galima rasti įdomesnių transakcijų, kurios atliktos ypač greitai, turi didelį įvesčių ir išvesčių skaičių bei buvo sumokamas didesnis transakcijos mokestis, kad įvykdyti transakcijas.

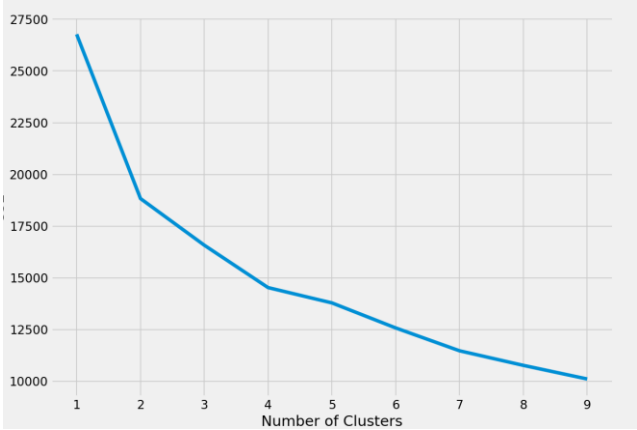
3.2. Klasterizavimo metodų pritaikymas

Galutiniam duomenų rinkiniui, kurį sudaro skirtingi rodikliai, pritaikysime klasterizavimo metodus. Pritaikomi skirtingi klasterizavimo metodai, siekiant palyginti metodų rezultatus.

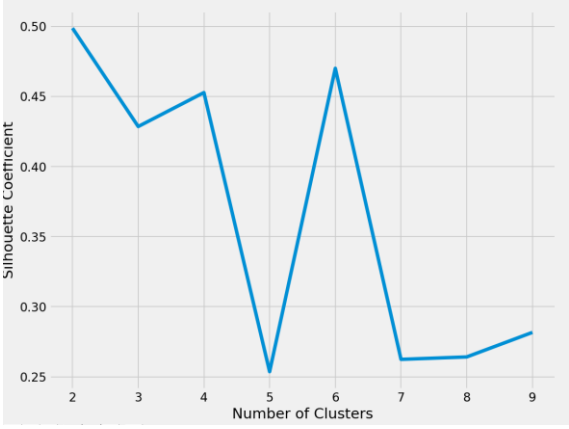
3.2.1. K-vidurkių metodo pritaikymas

K-vidurkių metodas ypatingas tuo, kad jame reikia nurodyti klasterių skaičių. Klasterių skaičių galima nurodyti rankiniu būdu ir kaskart iteruojant jį keisti, lyginti, kuris klasterių skaičius yra tinkamesnis. Kitas būdas yra pritaikyti klasterių skaičiaus nustatymo metodus naudojant alkūnės (angl. *elbow*) arba *Silhouette* koeficientą.

Duomenų rinkiniui pritaikome alkūnės metodą. Rezultate metodas rodo, kad 4 klasteriai paaiškintų daugumą taškų. Jeigu rinktumėmės daugiau nei 4 klasterius, tai turėtume daugiau smulkesnių klasterių. Duomenų rinkiniui pritaikius *Silhouette* koeficientą, gauname, kad 4 klasteriai pakankamai gerai paaiškina visą duomenų rinkinį. Kitas siūlomas klasterių skaičius būtų 6, tačiau matome, kad koeficiento reikšmės skirtumas yra nedidelis.



15 pav. Alkūnės metodo grafikas



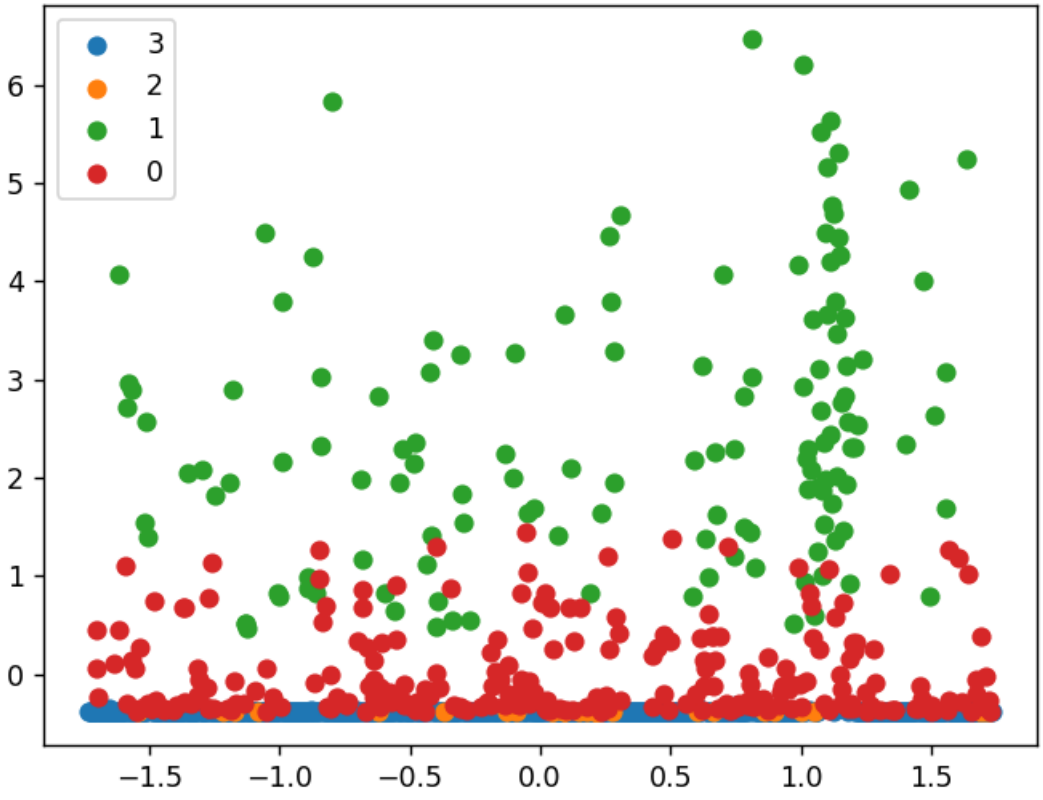
16 pav. *Silhouette* koeficiento grafikas

Pritaikę k-vidurkių metodą, gauname 4 klasterius (žr. 5 lentelėje).

5 lentelė. K-vidurkių metodo klasterių lentelė

Klasteris	Transakcijų skaičius
Klasteris 3	869
Klasteris 0	243
Klasteris 1	135
Klasteris 2	28

Rezultate matome, kad vyrauja vienas didysis klasterius, antras bei trečias klasteriai turi panašų skaičių taškų bei ketvirtas klasteris yra mažiausias, turi tik 28 taškus. Žemiau pateiktame paveikslėlyje (17 pav.) matosi kiekvieno klasterio taškai išskyrus antrąjį klasterį, nes jo taškai yra persidengę kartu su trečiuoju klasteriu.

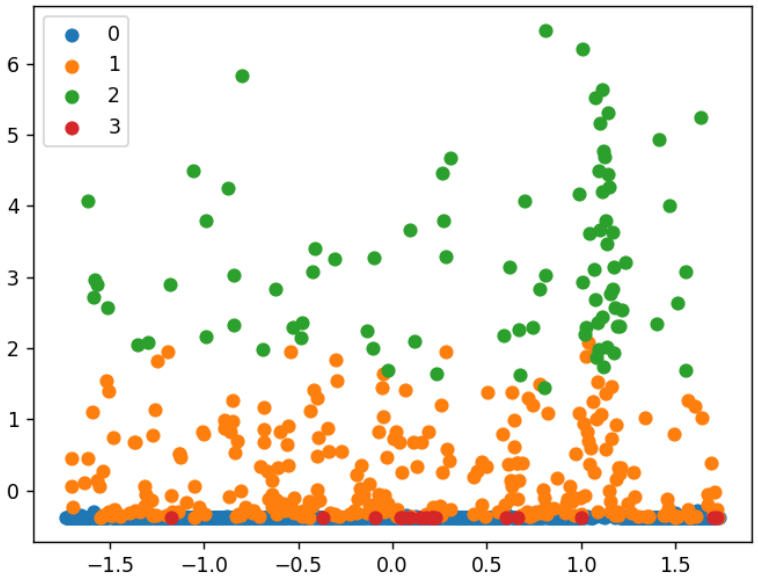


17 pav. K-vidurkių klasteriai grafike

3.2.2. Hierarchinių klasterizavimo metodų pritaikymas

Pritaikant hierarchinius klasterizavimo metodus reikia taip pat nurodyti klasterių skaičių. Šiuo atveju buvo naudojamas aglomeracijos metodas. Klasterių skaičius pasirinktas 4, kaip ir k-vidurkių metode. Šio metodo metu taškai yra padalinti į skirtingus klasterius bei jie kiekviename žingsnyje

yra jungiami, kol galiausiai lieka 4 skirtingi klasteriai. Žemiau pateiktame paveikslėlyje (18 pav.) matome panašų rezultatą pateikia ir hierarchinis klasterizavimas.



18 pav. Hierarchinio klasterizavimo rezultatai grafike

Lentelėje pateikti 4 duomenų klasteriai. Pirmasis klasteris yra pats didžiausias, apimantis didžiąją dalį taškų. Antrasis klasteris yra ganėtinai didelis taip pat. Trečiasis bei ketvirtasis klasteriai yra ganėtinai maži, apima 10% duomenų taškų.

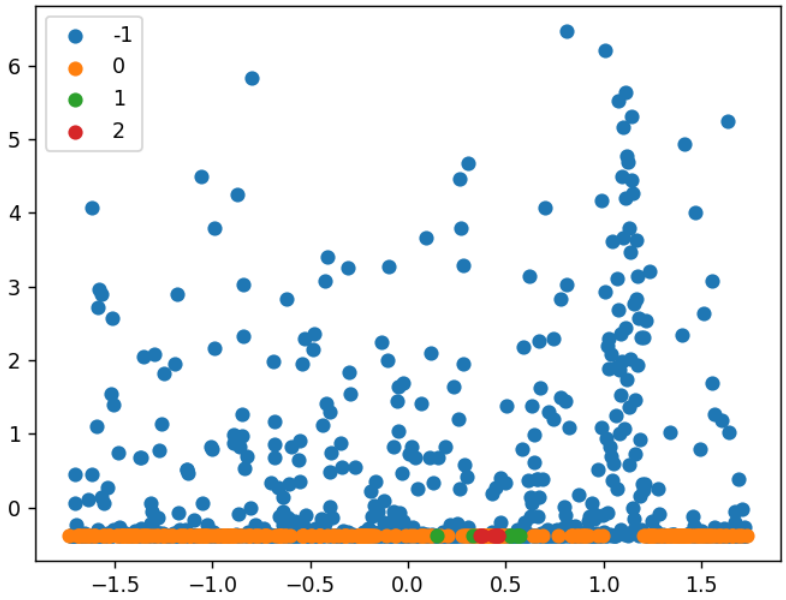
6 lentelė. Hierarchinio klasterizavimo rezultatai lentelėje

Klasteris	Transakcijų skaičius
Klasteris 0	891
Klasteris 1	279
Klasteris 2	88
Klasteris 3	17

Duomenis galima suskirstyti į klasterius naudojant tankiu grįstą klasterizavimą. Šis klasterizavimas yra vienas populiariausių. Duomenų rinkiniui pritaikome DBSCAN metodą. Šiuo atveju nėra nusakomas klasterių skaičius iš anksto. Nustatomi epsilon įvertis 0.25 bei mažiausių taškų klasteryje skaičius – 9.

7 lentelė. DBSCAN klasterizavimo rezultatai lentelėje

Klasteris	Transakcijų skaičius
Klasteris -1	955
Klasteris 0	299
Klasteris 1	12
Klasteris 2	9



19 pav. Klasterizavimo rezultatai DBSCAN grafike

Šiuo atveju pirmieji du (žr. 7 lentelėje) klasteriai apima daugumą klasterio taškų, trečiasis ir ketvirtasis yra labai maži klasteriai.

3.3. Transakcijų klasterizavimo palyginimas

Atlikus skirtingų tipų klasterizavimo metodus, galima pastebėti, kad rezultatai yra gana panašūs. Visi metodai buvo pritaikyti skaičiuojant 4 klasterius, siekiant palyginti juos tarpusavyje. Visi trys metodai pirmus du klasterius skirsto panašiai. Vyrauja pirma didžiausia taškų grupė, kurioje taškų skaičius svyruoja apie 900. Antrame klasteryje taškų yra 243 – 299, šis klasteris, sprendžiant iš taškų skaičiaus, irgi yra panašus visuose metoduose. Kiti du klasteriai yra skirtingi. K-vidurkių metodo trečiasis klasteris yra šiek tiek didesnis nei likusiųjų dviejų metodų. Ketvirtasis klasteris visuose metoduose yra mažiausias.

8 lentelė. Klasterizavimo rezultatų apibendrinimas

	Metodai		
	K-vidurkių (transakcijų skaičius)	Aglomeracijos (transakcijų skaičius)	DBSCAN (transakcijų skaičius)
Klasteris 1	869	891	955
Klasteris 2	243	279	299
Klasteris 3	135	88	12
Klasteris 4	28	17	9

Siekiant rasti tinkamiausią klasterizavimo metodą, palyginsime skirtingų metodų rezultatus.

3.3.1. Pirmojo klasterio palyginimas

Pirmąjį klasterį visuose metoduose sudaro didžiausias transakcijų grafų skaičius. K-vidurkių metode didžioji dalis transakcijų yra grafai, kurie neturi daug viršūnių (žr. 9 lentelėje). Trejuose kvartiliuose transakcijų grafo viršūnių skaičius siekia 23 (lentelėje *Number_of_nodes*). Vidutinis

grafo viršūnės laipsnis lygus 2 (lentelėje *Average_graph_degree*), vadinasi, dauguma transakcijų turi vieną arba dvi įvestis. Laikas transakcijų yra įvairus, vyrauja tiek greitos transakcijos, tiek labai ilgos.

9 lentelė. K-vidurkių metodo pirmojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	869	613	371	0	290	913	1274
Unnamed..0	869	615	371	2	292	915	1276
Number_of_nodes	869	90	369	5	11	23	5367
Number_of_edges	869	92	382	4	10	23	5586
Highest_graph_degree	869	17	43	2	2	7	273
Average_graph_degree	869	1.9	0.13	1.6	1.8	2	2.9
Fee_average_btc	869	0.00036	0.001	0.00000035	0.000018	0.00032	0.017
Average_input_counts	869	11	33	0.75	1	3.6	333
Average_output_counts	869	24	41	1.1	2	29	262
Average_input_value_btc	869	30	123	0.00028	0.69	16	2803
Max_input_value_btc	869	332	1029	0.0003	1.5	111	14839
Min_input_value_btc	869	1.6	9.1	0.0000031	0.0005	0.15	194
Average_transaction_time_diff_min	869	6054	16021	0	126	2519	132626
Block_time_std	869	18232	56034	0	319	8719	692423
Input_count_std	869	9	25	0	0	3.2	240
Output_count_std	869	52	114	0	0.32	37	874
Value_std	869	58	185	0.0000085	0.22	27	2989
Fee_std	869	0.00042	0.0014	0	0.0000062	0.00039	0.023
Difference_newest_oldest_transaction_dates_in_min	869	49572	147716	0	445	21861	1858130
Max_number_of_tran_per_day	869	13	35	1	4	10	612
Max_time_min	869	49664	147708	0	496	21866	1858132
Min_time_min	869	91	475	0	6	32	9327

Aglomeracijos metodas pirmajame klasteryje išskyrė 891 transakcijų grafus. Šiame klasteryje transakcijų grafai turi taip pat vidutiniškai vieną ar dvi transakcijos įvestis. Viršūnių skaičius trejuose kvartiliuose siekia 24. Transakcijų laikai taip pat svyruoja panašiai, yra tiek ilgesnių tiek greitesnių transakcijų.

10 lentelė. Aglomeracijos metodo pirmojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	891	616	372	0	290	918	1274
Unnamed..0	891	618	372	2	292	920	1276
Number_of_nodes	891	123	554	5	11	24	8437
Number_of_edges	891	124	571	4	10	24	8675
Highest_graph_degree	891	21	58	2	2	7	483
Average_graph_degree	891	1.9	0.13	1.6	1.8	2	2.8
Fee_average_btc	891	0.00039	0.001	0.00000035	0.000019	0.00034	0.017
Average_input_counts	891	13	38	0.75	1	3.8	343
Average_output_counts	891	25	48	1.1	2	29	725
Average_input_value_btc	891	29	121	0.00028	0.7	16	2803
Max_input_value_btc	891	576	2717	0.0003	1.5	132	32234
Min_input_value_btc	891	1.6	9	0.0000031	0.00044	0.13	194
Average_transaction_time_diff_min	891	8639	28115	0	133	2996	255447
Block_time_std	891	25760	87262	0	338	9790	939138
Input_count_std	891	11	31	0	0	3.6	240
Output_count_std	891	55	122	0	0.32	38	878
Value_std	891	64	200	0.0000085	0.23	30	2989
Fee_std	891	0.00045	0.0014	0	0.0000068	0.00042	0.023
Difference_newest_oldest_transaction_dates_in_min	891	68407	219782	0	514	27142	1976877
Max_number_of_tran_per_day	891	15	46	1	4	10	626
Max_time_min	891	68516	219822	0	539	27157	1976894
Min_time_min	891	109	702	0	6	32	15595

DBSCAN metode didžiausias klasteris turi 955 transakcijų grafus. Šiame klasteryje yra skirtingo dydžio grafai, vidutinis viršūnių skaičius lygus net 43 228 (žr. 11 lentelėje). Pirmieji du kvartiliai turi iki 13 viršūnių, tačiau kiti kvartiliai turi daug daugiau viršūnių. Vidutinis įvesčių skaičius siekia 102 (lentelėje *Average_input_counts*). Transakcijų laiko rodikliai rodo, kad transakcijos vykdomos skirtingu dažnumu. Panašu, kad šiame klasteryje yra skirtingo tipo transakcijų grafai.

11 lentelė. DBSCAN metodo pirmojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	955	643	363	1	344	958	1273
Unnamed..0	955	645	363	3	346	960	1275
Number_of_nodes	955	43228	96153	5	13	22301	583767
Number_of_edges	955	62116	144890	4	13	24972	910862
Highest_graph_degree	955	301	374	2	3	649	1038
Average_graph_degree	955	2.2	0.54	1.6	1.9	2.2	5.6
Fee_average_btc	955	0.0019	0.0049	0.00000035	0.00013	0.0025	0.12
Average_input_counts	955	102	122	0.75	1.8	207	565
Average_output_counts	955	41	61	1.1	11	50	1113
Average_input_value_btc	955	28	117	0.0011	1.6	15	2803
Max_input_value_btc	955	9986	16009	0.0032	30	17726	45493
Min_input_value_btc	955	1.4	8.7	0.00000001	0.000005	0.0023	194
Average_transaction_time_diff_min	955	16760	63296	0.000046	418	5424	697907
Block_time_std	955	80788	172395	10	2118	93498	1544979
Input_count_std	955	87	101	0	1.2	197	358
Output_count_std	955	113	234	0	20	148	6195
Value_std	955	105	196	0.00061	4.2	133	2989
Fee_std	955	0.0037	0.0094	0	0.00012	0.0037	0.19
Difference_newest_oldest_transaction_dates_in_min	955	685594	1009319	0	5084	1126212	4337221
Max_number_of_tran_per_day	955	2240	4808	1	5	1235	29205
Max_time_min	955	667534	994845	15	4927	1101785	4337223
Min_time_min	955	122	1747	0.067	1.2	19	50277

3.3.2. Antrojo klasterio palyginimas

K-vidurkių metodas antrajame klasteryje (žr. 12 lentelėje) turi 243 transakcijų grafus. Šiame klasteryje transakcijų grafai turi daug daugiau viršūnių, yra sudėtingesni, vidutinis viršūnių skaičius siekia 33 596 (lentelėje *Number_of_nodes*). Šie transakcijų grafai yra sudaryti didesnėms bitkoino sumoms, vidutinė vertė siekia 5,4 bitkoinus (lentelėje *Average_inpu_value_btc*). Taip pat šiuose grafuose yra ypač greitų transakcijų, vidutinė mažiausia trukmė tarp transakcijų (lentelėje *Min_time_min*) siekia 2,5 minutės.

12 lentelė. K-vidurkių metodo antrojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	243	654	364	11	382	975	1272
Unnamed..0	243	656	364	13	384	977	1274
Number_of_nodes	243	33596	38939	33	4610	54791	155100
Number_of_edges	243	39661	48437	32	4864	60738	216630
Highest_graph_degree	243	630	209	11	493	787	1038
Average_graph_degree	243	2.2	0.31	1.9	2.1	2.3	4.8
Fee_average_btc	243	0.0047	0.0089	0.00041	0.0021	0.0041	0.12
Average_input_counts	243	251	94	5.3	193	292	565
Average_output_counts	243	48	91	1.1	21	48	1113
Average_input_value_btc	243	5.4	12	0.3	1.8	4.1	101
Max_input_value_btc	243	16475	14820	49	2625	21703	45493
Min_input_value_btc	243	0.000018	0.00013	0.00000001	0.0000034	0.0000055	0.0017
Average_transaction_time_diff_min	243	5560	14867	11	969	4303	181953
Block_time_std	243	77731	104130	674	14309	107565	903102
Input_count_std	243	210	53	3.9	187	243	358
Output_count_std	243	214	403	1.5	121	236	6195
Value_std	243	138	175	3.5	35	186	1293
Fee_std	243	0.0086	0.017	0.00051	0.0024	0.0072	0.19
Difference_newest_oldest_transaction_dates_in_min	243	960943	848210	194	205847	1851705	4337221
Max_number_of_tran_per_day	243	2119	2361	4	274	3590	10485
Max_time_min	243	960945	848209	208	205848	1851706	4337223
Min_time_min	243	2.5	3	0.067	0.67	2.9	19

Aglomeracijos metodo antrajame klasteryje yra 279 transakcijų grafai, kurių vidutinis viršūnių skaičius yra 51 250 (žr. 13 lentelėje). Vidutinis transakcijų grafo viršūnių laipsnis siekia 2 (lentelėje *Average_graph_degree*), toks pats įvertis yra k-vidurkių metodo antrajame klasteryje. Tai parodo, kad transakcijos yra ganėtinai įprastos, nesudėtingos. Šios transakcijos atliekamos taip pat greičiau, vidutiniškai trumpiausias laikas tarp transakcijų siekia 2 minutes.

13 lentelė. Aglomeracijos metodo antrojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	279	647	356	11	372	975	1272
Unnamed..0	279	649	356	13	374	977	1274
Number_of_nodes	279	51250	53448	33	6482	90798	209260
Number_of_edges	279	70049	80687	32	6644	112587	315699
Highest_graph_degree	279	664	210	11	536	817	1038
Average_graph_degree	279	2.4	0.75	1.9	2.1	2.4	5.6
Fee_average_btc	279	0.0044	0.0083	0.00028	0.0021	0.0037	0.12
Average_input_counts	279	243	94	5.3	180	280	565
Average_output_counts	279	50	77	1.6	21	58	1113
Average_input_value_btc	279	3.2	3.6	0.3	1.5	3.3	37
Max_input_value_btc	279	18827	15743	28	3000	22516	45493
Min_input_value_btc	279	0.000016	0.00012	0.00000001	0.0000030	0.0000055	0.0017
Average_transaction_time_diff_min	279	4697	13841	0.071	858	3638	181953
Block_time_std	279	90266	104274	674	19127	125312	903102
Input_count_std	279	202	64	3.9	181	242	358
Output_count_std	279	188	373	5.9	112	207	6195
Value_std	279	114	94	1.9	37	163	718
Fee_std	279	0.0086	0.016	0.00034	0.0026	0.0079	0.19
Difference_newest_oldest_transaction_dates_in_min	279	1154052	874040	194	271348	1970225	4337221
Max_number_of_tran_per_day	279	2851	3055	4	354	4641	11518
Max_time_min	279	1132846	877351	208	253516	1957015	4337223
Min_time_min	279	2	2.5	0.067	0.63	2.1	19

Tankiu grįsto metodo trečiajame klasteryje yra 299 transakcijų grafai (žr. 14 lentelėje). Šis klasteris kitaip negu kitų dviejų metodų, turi grafus, kurie turi vidutiniškai 12 viršūnių. Viršūnių vidutinis laipsnis siekia 2, taip pat kaip kituose metoduose. Šiame klasteryje sugrupuotos transakcijos turi mažą įvesčių bei išvesčių skaičius, vidutiniškai 1.2 bei 3.6.

14 lentelė. DBSCAN metodo antrojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	299	606	392	0	258	969	1274
Unnamed..0	299	608	392	2	260	971	1276
Number_of_nodes	299	12	1.8	11	11	11	30
Number_of_edges	299	11	1.8	10	10	10	29
Highest_graph_degree	299	2.2	0.72	2	2	2	11
Average_graph_degree	299	1.8	0.016	1.8	1.8	1.8	1.9
Fee_average_btc	299	0.000052	0.00009	0.0000035	0.000012	0.000041	0.00047
Average_input_counts	299	1.2	0.66	1	1	1.1	7
Average_output_counts	299	3.6	3.2	1.4	2	3.5	20
Average_input_value_btc	299	2.2	4.4	0.00028	0.15	1.9	27
Max_input_value_btc	299	6	15	0.0003	0.25	4	120
Min_input_value_btc	299	0.38	0.66	0.0000055	0.0049	0.51	4.3
Average_transaction_time_diff_min	299	964	1896	0	31	745	11495
Block_time_std	299	2545	5208	0	69	1998	38077
Input_count_std	299	0.47	1.6	0	0	0.36	15
Output_count_std	299	2.5	5.8	0	0	1.9	38
Value_std	299	2.1	5.7	0.0000085	0.022	1.1	45
Fee_std	299	0.00003	0.000084	0	0.0000019	0.00002	0.00094
Difference_newest_oldest_transaction_dates_in_min	299	4603	10982	0	60	3257	77786
Max_number_of_tran_per_day	299	7.1	2.6	2	5	10	15
Max_time_min	299	4628	10984	0	70	3298	77799
Min_time_min	299	25	46	0	4.4	24	351

3.3.3. Trečiojo klasterio palyginimas

Trečiajame k-vidurkių metodo klasteryje vyrauja transakcijos, kurios turi didelį skaičių viršūnių, vidutiniškai net 244 767 (žr. 15 lentelėje). Šios transakcijos išsiskiria tuo, kad yra nedidelės vertės, tačiau turi didelį kiekį įvesčių ir išvesčių, vidurkiai siekia net 196 bei 67 (lentelėje *Average_input_counts* bei *Average_output_counts*), tačiau transakcijų suma vidutiniškai siekia tik

1.6 bitkoino (lentelėje *Average_input_value_btc*). Taip pat šiame klasteryje yra transakcijų, kurios yra patvirtintos tame pačiame arba kitame bloke, nes transakcijų minimalus laiko skirtumas siekia tik 0.71 minutės.

15 lentelė. K-vidurkių metodo trečiojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	135	742	347	43	450	1042	1238
Unnamed..0	135	744	347	45	452	1044	1240
Number_of_nodes	135	244767	118304	72256	156888	310731	583767
Number_of_edges	135	367455	183943	106897	229244	468670	910862
Highest_graph_degree	135	892	165	357	920	1002	1038
Average_graph_degree	135	3.1	0.83	2.4	2.5	3.2	5.6
Fee_average_btc	135	0.0026	0.00068	0.0014	0.0022	0.003	0.0046
Average_input_counts	135	196	61	90	155	249	299
Average_output_counts	135	67	42	16	24	95	149
Average_input_value_btc	135	1.6	0.61	0.56	1.2	2	3.8
Max_input_value_btc	135	38854	10867	11056	32234	45493	45493
Min_input_value_btc	135	0.0000023	0.0000014	0.00000001	0.00000001	0.0000030	0.0000047
Average_transaction_time_diff_min	135	1341	2089	0.000046	0.0057	1822	15028
Block_time_std	135	143736	68917	25113	93498	202136	307914
Input_count_std	135	183	64	25	166	228	261
Output_count_std	135	110	30	40	97	129	185
Value_std	135	119	52	12	86	142	284
Fee_std	135	0.0077	0.0042	0.0029	0.004	0.01	0.024
Difference_newest_oldest_transaction_dates_in_min	135	2463548	849109	787760	1970227	3246386	3861009
Max_number_of_tran_per_day	135	11966	6155	125	8760	15540	29205
Max_time_min	135	2334932	980555	1758	1942782	3239593	3861009
Min_time_min	135	0.71	0.3	0.067	0.43	1	1.1

Aglomeracijos metodo trečiajame klasteryje yra 88 transakcijų grafai (žr. 16 lentelėje). Šie grafai taip pat turi didelį skaičių viršūnių, siekia net 305 432. Transakcijų įvesčių ir išvesčių skaičius vidutiniškai siekia 202 bei 62. Šiame klasteryje transakcijų suma vidutiniškai siekia tik 1.6 bitkoino. Žinant, kad transakcijų įvesčių kiekis yra labai didelis, tai ganėtinai maža transakcijų vidutinė suma.

16 lentelė. Aglomeracijos metodo trečiojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	88	797	345	43	514	1053	1238
Unnamed..0	88	799	345	45	516	1055	1240
Number_of_nodes	88	305432	99888	156094	227919	375216	583767
Number_of_edges	88	450792	174533	196115	315180	585205	910862
Highest_graph_degree	88	959	74	680	920	1002	1038
Average_graph_degree	88	2.9	0.36	2.4	2.6	3.2	3.9
Fee_average_btc	88	0.0027	0.00068	0.0015	0.0023	0.003	0.0046
Average_input_counts	88	202	50	100	162	246	289
Average_output_counts	88	62	34	16	27	92	131
Average_input_value_btc	88	1.6	0.46	0.82	1.2	1.9	3
Max_input_value_btc	88	42863	6266	21485	45136	45493	45493
Min_input_value_btc	88	0.0000019	0.0000015	0.00000001	0.00000001	0.0000030	0.0000043
Average_transaction_time_diff_min	88	1355	2343	0.000046	0.0025	1481	15028
Block_time_std	88	144188	65840	25113	96638	193776	307914
Input_count_std	88	197	39	77	175	229	250
Output_count_std	88	113	19	69	98	125	185
Value_std	88	125	38	60	100	145	246
Fee_std	88	0.0079	0.0032	0.0031	0.0053	0.0099	0.015
Difference_newest_oldest_transaction_dates_in_min	88	2749619	858913	989633	2006152	3809133	3861009
Max_number_of_tran_per_day	88	15141	4560	4064	12240	17237	29205
Max_time_min	88	2619549	996940	1974	1999952	3806293	3861009
Min_time_min	88	0.69	0.3	0.067	0.42	1	1.1

Trečiasis DBSCAN metodo klasteris turi tik 12 transakcijų (žr. 17 lentelėje). Šiame klasteryje transakcijų grafo viršūnių vidutinis skaičius siekia 11. Transakcijose vidutiniškai siunčiama 2.5 bitkoino. Vidutinis įvesčių bei išvesčių skaičius yra atitinkamai 1 bei 4. Šios 12 transakcijų yra trumpos bei lėtos, vidutinis trumpiausias laikas tarp transakcijų siekia 2 022 minutes.

17 lentelė. DBSCAN metodo trečiojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	12	791	15	773	776	804	807
Unnamed..0	12	793	15	775	778	806	809
Number_of_nodes	12	11	0	11	11	11	11
Number_of_edges	12	10	0	10	10	10	10
Highest_graph_degree	12	2	0	2	2	2	2
Average_graph_degree	12	1.8	0	1.8	1.8	1.8	1.8
Fee_average_btc	12	0.000018	0.0000012	0.000016	0.000017	0.000018	0.00002
Average_input_counts	12	1	0	1	1	1	1
Average_output_counts	12	3.7	0.53	2.9	3.3	4	4.6
Average_input_value_btc	12	2.5	0.025	2.4	2.5	2.5	2.5
Max_input_value_btc	12	9.9	0.044	9.8	9.8	9.9	9.9
Min_input_value_btc	12	0.99	0.019	0.95	0.98	1	1
Average_transaction_time_diff_min	12	2405	1.5	2403	2403	2407	2407
Block_time_std	12	7390	6.9	7381	7386	7393	7402
Input_count_std	12	0	0	0	0	0	0
Output_count_std	12	1.5	0.65	0.84	0.99	1.9	3.1
Value_std	12	2.9	0.024	2.8	2.9	2.9	2.9
Fee_std	12	0.0000043	0.000001	0.0000027	0.0000038	0.0000047	0.0000064
Difference_newest_oldest_transaction_dates_in_min	12	754	26	719	733	781	786
Max_number_of_tran_per_day	12	1	0	1	1	1	1
Max_time_min	12	2776	20	2756	2756	2786	2805
Min_time_min	12	2022	13	1998	2019	2028	2037

3.3.4. Ketvirtojo klasterio palyginimas

Ketvirtasis klasteris yra mažiausias visuose metoduose. K-vidurkių metode šiame klasteryje yra 28 transakcijų grafai (žr. 18 lentelėje). Vidutiniškai šiuose grafuose yra 17 viršūnių, tačiau siunčiamos didesnės bitkoino sumos, vidutiniškai apie 13 bitkoinų. Šios transakcijos nėra atliekamos labai greitai bei labai dažnai, vidutiniškai yra apie 4 transakcijas per dieną (lentelėje *Max_number_of_tran_per_day*).

18 lentelė. K-vidurkių metodo ketvirtojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	28	712	311	70	599	898	1269
Unnamed..0	28	714	311	72	601	900	1271
Number_of_nodes	28	17	11	11	11	16	50
Number_of_edges	28	16	11	10	10	16	49
Highest_graph_degree	28	4.5	4.7	2	2	5	20
Average_graph_degree	28	1.9	0.053	1.8	1.8	1.9	2
Fee_average_btc	28	0.00073	0.0018	0.000022	0.00017	0.00043	0.0095
Average_input_counts	28	2.5	2.6	1	1.1	2.1	10
Average_output_counts	28	13	18	1.9	2.7	14	94
Average_input_value_btc	28	13	13	0.0053	0.99	29	32
Max_input_value_btc	28	74	92	0.0063	1.4	127	453
Min_input_value_btc	28	0.049	0.066	0.0000055	0.00042	0.13	0.2
Average_transaction_time_diff_min	28	341098	138453	124013	241798	404698	697907
Block_time_std	28	853103	369523	153426	558989	1126309	1544979
Input_count_std	28	2.3	4.4	0	0.32	2	22
Output_count_std	28	31	55	0	0.75	40	291
Value_std	28	26	28	0.00061	0.65	52	113
Fee_std	28	0.0016	0.005	0.000016	0.00031	0.00059	0.026
Difference_newest_oldest_transaction_dates_in_min	28	1679371	483593	459605	1571225	1919062	2352323
Max_number_of_tran_per_day	28	3.7	1.8	1	2.8	4.2	9
Max_time_min	28	1681820	477532	505111	1571231	1919081	2352338
Min_time_min	28	2449	9824	3.2	17	42	50277

Aglomeracijos metode ketvirtasis klasteris turi 17 transakcijų grafų. Šiame klasteryje vyrauja dar didesnės transakcijų sumos, vidutiniškai siunčiama apie 18 bitkoinų (žr. 19 lentelėje). Įvesčių bei

išvesčių skaičius yra ganėtinai mažas, siekia vidutiniškai atitinkamai 2 bei 18. Transakcijos yra atliekamos lėčiau, vidutiniškai 4 transakcijos per dieną.

19 lentelė. Aglomeracijos metodo ketvirtojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	17	754	255	206	654	859	1269
Unnamed..0	17	756	255	208	656	861	1271
Number_of_nodes	17	15	6	11	11	18	34
Number_of_edges	17	14	6	10	10	17	33
Highest_graph_degree	17	3.6	1.8	2	2	5	7
Average_graph_degree	17	1.9	0.04	1.8	1.8	1.9	1.9
Fee_average_btc	17	0.00092	0.0023	0.000086	0.00017	0.00032	0.0095
Average_input_counts	17	1.8	0.57	1.1	1.2	2.1	3.2
Average_output_counts	17	18	22	1.9	4.9	14	94
Average_input_value_btc	17	18	13	0.03	4.7	29	32
Max_input_value_btc	17	81	54	0.092	29	127	127
Min_input_value_btc	17	0.06	0.065	0.000023	0.00027	0.13	0.13
Average_transaction_time_diff_min	17	424486	111385	280079	357672	433162	697907
Block_time_std	17	1011717	381193	153426	771184	1126322	1544979
Input_count_std	17	1.3	0.96	0.32	0.42	1.8	2.8
Output_count_std	17	45	66	0	14	40	291
Value_std	17	31	23	0.023	13	52	53
Fee_std	17	0.0023	0.0064	0.000048	0.00047	0.00058	0.026
Difference_newest_oldest_transaction_dates_in_min	17	1840679	401338	459605	1879637	1919064	2352323
Max_number_of_tran_per_day	17	4	1.9	2	3	4	9
Max_time_min	17	1843659	390570	509882	1879641	1919081	2352338
Min_time_min	17	2980	12188	3.2	18	32	50277

Ketvirtajame DBSCAN klasteryje yra tik 9 transakcijų grafai (žr. 20 lentelėje). Šie grafai turi vidutiniškai 10 viršūnių. Tokiose transakcijose pervedami vidutiniškai 6.6 bitkoinai. Visos transakcijų grafų mažiausias laiko skirtumas tarp transakcijų siekia 67 minutes. Transakcijų nėra įvykdoma daug, vidutiniškai 4 per dieną.

20 lentelė. DBSCAN metodo ketvirtojo klasterio apžvalga

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
X	9	813	53	692	828	842	847
Unnamed..0	9	815	53	694	830	844	849
Number_of_nodes	9	10	0	10	10	10	10
Number_of_edges	9	11	0	11	11	11	11
Highest_graph_degree	9	4	0	4	4	4	4
Average_graph_degree	9	2.2	0	2.2	2.2	2.2	2.2
Fee_average_btc	9	0.00031	0.00000023	0.00031	0.00031	0.00031	0.00031
Average_input_counts	9	2.2	0	2.2	2.2	2.2	2.2
Average_output_counts	9	175	0.03	175	175	175	175
Average_input_value_btc	9	5.3	0.000021	5.3	5.3	5.3	5.3
Max_input_value_btc	9	6.6	0	6.6	6.6	6.6	6.6
Min_input_value_btc	9	0.0012	0.00017	0.001	0.0011	0.0014	0.0015
Average_transaction_time_diff_min	9	2257	0	2257	2257	2257	2257
Block_time_std	9	2431	0	2431	2431	2431	2431
Input_count_std	9	1.8	0	1.8	1.8	1.8	1.8
Output_count_std	9	381	0.015	381	381	381	381
Value_std	9	2.2	0.000056	2.2	2.2	2.2	2.2
Fee_std	9	0.00066	0.00000012	0.00066	0.00066	0.00066	0.00066
Difference_newest_oldest_transaction_dates_in_min	9	6802	0	6802	6802	6802	6802
Max_number_of_tran_per_day	9	4	0	4	4	4	4
Max_time_min	9	6869	0	6869	6869	6869	6869
Min_time_min	9	67	0	67	67	67	67

Atlikus visų metodų klasterių aprašomosios analizės palyginimą, galime matyti, kad k-vidurkių bei aglomeracijos metodai pateikia ganėtinai panašius rezultatus. DBSCAN metodas šiuo atveju pateikė kitokius rezultatus. DBSCAN metode yra klasterių, kurie apima skirtingo tipo transakcijų grafus,

tiek mažesnius, tiek didesnius bei priskiria šiuos grafus prie to pačio klasterio dėl kitų savybių. Tačiau DBSCAN metode vyrauja didesnė variacija tarp rodiklių. Minimalios tiek maksimalios reikšmės skiriasi ženkliai, visuose klasteriuose matomos didelės variacijos. Tuo tarpu k-vidurkių bei aglomeracijos metodai yra labai panašūs. Jų klasterių apibūdinimai yra labai artimi. K-vidurkių metodo klasteriai yra šiek tiek labiau apibendrinti, netgi paskutinis klasteris turi daugiau transakcijų grafų nei aglomeracijos metodo paskutinis klasteris. Atlikus klasterių palyginamąją analizę matome, kad aglomeracijos bei k-vidurkių metodai yra tinkamesni. Siekiant turėti labiau apibendrintus klasterius naudosime k-vidurkių metodo rezultatą.

3.4. Transakcijų vertinimo koeficientas

Siekiant įvertinti bitkoino transakcijas, galima paskaičiuoti transakcijų vertinimo koeficientą. Šis koeficientas įvertintų transakcijos ypatybes. Jeigu bitkoino transakcija yra vykdoma pernelyg greitai, ar yra sudaryta iš neįprastai daug įvesčių, galima būtų daryti prielaidą, kad ta transakcija yra labiau įtartina nei kitos. Transakcijų ypatybes parodo skirtingi rodikliai, tačiau dauguma pinigų plovimo schemų naudoja panašius modelius. Vienas populiariausių metodų yra transakcijų sumaišymo paslaugos. Šis metodas skaido didesnę bitkoino monetą į daug mažesnių monetų, kurios pervedamos į skirtingus adresus, vėliau vėlgi smulkinamos, vėliau stambinamos, kol galiausiai nauja moneta, sudaryta iš sumaišytų monetų, yra pervedama į savininko sąskaitą. Tokiu būdu bitkoino monetos yra sumaišomos ir, esant dideliam transakcijų skaičiui, sunkiau atskirti, kokia yra monetų prigimtis.

Transakcijų vertinimo koeficientas gali padėti įvertinti kiekvieną transakciją transakcijų grafe. Siekiant įvertinti transakciją išskiriamos keletas pagrindinių taisyklių:

1. Visos transakcijos iš pradžių turi koeficientą lygų 1.
2. Jeigu transakcija sudaryta iš daugiau nei 10 įvesčių, koeficientas yra mažinamas 0,1 dydžiu.
3. Jeigu transakcija sudaryta iš daugiau nei 10 išvesčių, koeficientas yra mažinamas 0,1 dydžiu.
4. Jeigu transakcijos laiko skirtumas su buvusiąja transakcija yra mažesnis nei 60 minučių, koeficientas yra mažinamas 0,1 dydžiu.
5. Jeigu transakcijos mokesčio dydis yra didesnis nei 140 000 satošių, tuomet koeficientas yra mažinamas 0,1 dydžiu.
6. Galiausiai yra paskaičiuojamas svertinis vidurkis visų grafo transakcijų, kur svoris yra lygus transakcijų sumai.

Suskaičiuosime transakcijų vertinimo koeficientą vienai iš transakcijų iš 700 000 bloko.

21 lentelė. Transakcijos duomenys su transakcijų vertinimo koeficiento rezultatu

Transakcijos maiša	Įvesties transakcijos maiša	Laiko žyma	Įvesčių skaičius	Išvesčių skaičius	Mokestis	Įvesties suma	Laiko skirtumas	Koeficientas
2b9766683f0cc3c0733	e5c8583a6e03ff768	2021-09-11 04:14:32	1	1	490	7988	Nan	1
e5c8583a6e03ff76892	9e873a483e3d26db	2021-09-03 01:23:01	1	2	420	639878	11691	1
9e873a483e3d26db1a	e72c073edb322cdd	2021-09-02 20:48:09	1	94	33964	38953894	274	0,9
e72c073edb322cddae6	3a27cc15d254c05b5	2021-09-02 20:02:21	1	1	1456	38955350	45	0,9
3a27cc15d254c05b5e6	75436bd1012c8147f	2021-01-07 04:52:54	2	2	22704	100000000	343569	1
75436bd1012c8147f83	54bd551523d15bb8	2021-01-07 04:08:03	1	11	47652	193059192	44	0,8
54bd551523d15bb8de	ad6522ce82518a0b	2021-01-07 03:09:07	1	9	41631	214666823	58	0,9
ad6522ce82518a0ba7	a10ae1d87c5c84e2	2021-01-07 02:15:25	1	6	32323	279129146	53	0,9
a10ae1d87c5c84e224	c294e1ea553e85bb	2021-01-07 00:01:04	1	9	41633	611828779	134	1
c294e1ea553e85bb63	2fb889dbee422f0ec	2021-01-06 22:04:09	1	6	32680	699481459	116	1

Lentelėje (žr. 21 lentelę) pateiktas transakcijos bei jos įvesčių pavyzdys. Naudojant transakcijų vertinimo koeficientą yra įvertinama kiekviena transakcijos medžio transakcija. Pati pirmoji transakcija turi tik vieną įvestį bei vieną išvestį, mokestis yra mažas bei laiko skirtumas tarp laiko žymų yra didelis, todėl transakcijos vertinimo koeficientas išlieka lygus 1. Trečioji transakcija turi didelį išvesčių skaičių, net 94, todėl transakcija yra mažinama 0,1 įverčiu. Šeštoji transakcija yra mažinama 0,2 įverčiu todėl, kad išvesčių skaičius yra didesnis nei 10 bei transakcijos laiko žymos skirtumas yra mažesnis nei 60 minučių. Tokiu būdu yra įvertinamos visos transakcijų medžio transakcijos, šiame tyrime analizuojamos 10 žingsnių transakcijos, todėl vertinamos būtent jos. Galiausiai paskaičiuojamas svertinis vidurkis, kurio svoris yra lygus transakcijos sumai. Šios transakcijos vertinimo koeficientas yra lygus 0,956.

Taip gaunamas transakcijų įvertinimas. Jeigu transakcijos grafe yra įprastos, vykdomos ne per dažnai bei labiausiai panašios į tam tikrą ekonominę veiklą, tuomet transakcijų vertinimo koeficientas yra aukštas. Jeigu transakcijos grafe yra sudėtingos struktūros, turi daug įvesčių bei išvesčių arba atliekamos ganėtinai greitai, tuomet transakcijos turi žemesnį koeficientą bei daroma prielaida, kad jos yra labiau įtartinos. Atlikus 700 000 bitkoino bloko koeficiento paskaičiavimus, matome, kad bloke yra skirtingo tipo transakcijos, žemiausias koeficientas yra 0.624, o didžiausias 1. Viso bloke yra 23 transakcijų medžiai, kurie yra įvertinti koeficientu lygiu 1, tai sudaro 1.8% visų transakcijų bloke. Tokios transakcijos yra įprastos, niekuo neišsiskiria, atliekamos ne dažnai bei lėšos pervedamos dažniausiai vienam gavėjui. Mažiausias transakcijų vertinimo koeficientas yra 0.624. Šiame bloke yra 10 transakcijų, kurių vertinimo koeficientas yra mažesnis nei 0.7. Tokie transakcijų grafai turi daug viršūnių, daug įvesčių bei transakcijos yra atliekamos ganėtinai greitai, kai kurios transakcijos yra netgi tvirtinamos tame pačiame bloke.

```
Koeficientas
       n  missing distinct     Info     Mean      Gmd      .05      .10      .25      .50      .75
    1275        0     1085    0.999   0.8841  0.06637   0.7864   0.8112   0.8520   0.8885   0.9206
     .90      .95
  0.9632   0.9846

lowest : 0.6244230 0.6655083 0.6662404 0.6676066 0.6682187, highest: 0.9996952 0.9998398 0.9998851 0.9999187 1.0000000
```

20 pav. Transakcijų vertinimo koeficiento apžvalga

Pateikti duomenys (20 pav.) rodo, kad vidutinis koeficiento įvertis lygus 0.8841. Pirmasis kvartilis rodo, kad vertinimo koeficientas lygus 0.852 arba mažiau. Ketvirtajame kvartilyje vertinimo koeficientas lygus 0.9206 arba daugiau. Vertinant šio bloko duomenis, galima daryti prielaidą, kad jeigu vertinimo koeficientas yra mažesnis nei 0.75, tuomet vertėtų tuos transakcijų medžius ištirti nuodugniau.

Galima palyginti klasterizavimo rezultatus kartu su vertinimo koeficientu. K-vidurkių metodas išskyrė 4 skirtingus klasterius. Pirmasis, didžiausias klasteris, turi 869 taškus. Šiame klasteryje vertinimo koeficientas pasiskirstęs panašiai, kaip ir visame duomenų rinkinyje. Vyrauja daugumoje aukštu koeficientu įvertinti grafai, tačiau yra ir keletas žemesnio koeficiento transakcijų grafų. Šiame klasteryje yra 17 transakcijų grafų, kurių vertinimo koeficientas yra mažesnis nei 0.75.

```
Koeficientas
       n  missing distinct     Info     Mean      Gmd      .05      .10      .25      .50      .75      .90      .95
     869        0      693    0.998   0.8994  0.06518   0.7933   0.8170   0.8705   0.9000   0.9415   0.9722   0.9891

lowest : 0.6244230 0.6655083 0.7047997 0.7052325 0.7061170, highest: 0.9989253 0.9996952 0.9998398 0.9998851 1.0000000
```

21 pav. Transakcijų vertinimo koeficiento pirmajame klasteryje apžvalga

Antrame klasteryje yra 243 nariai. Šiame klasteryje yra tik keletas transakcijų grafų, kurių vertinimo koeficientas didesnis nei 0.9. Didžiausia dalis transakcijų šiame klasteryje turi vertinimo koeficientą tarp 0.8 bei 0.9. Taip pat šiame klasteryje yra tik 6 transakcijos, kurių vertinimo koeficientas yra mažesnis nei 0.75.

```
Koeficientas
       n  missing distinct     Info     Mean      Gmd      .05      .10      .25      .50      .75      .90      .95
     243        0      233        1   0.8517  0.03515   0.7956   0.8118   0.8407   0.8609   0.8713   0.8814   0.8901

lowest : 0.6676066 0.6843750 0.6998012 0.7040808 0.7068545, highest: 0.9020466 0.9143856 0.9170541 0.9187889 0.9307575
```

22 pav. Transakcijų vertinimo koeficiento antrajame klasteryje apžvalga

Trečiajame klasteryje yra 135 taškai. Šiame klasteryje tik vienas grafas buvo įvertintas aukščiau nei 0.9 koeficientu. Daugiau transakcijų grafų, kurie buvo įvertinti mažiau nei 0.87. Šiame klasteryje yra 13 transakcijų grafų, kurių vertinimo koeficientas yra mažesnis nei 0.75.

```
Koeficientas
       n  missing distinct     Info     Mean      Gmd      .05      .10      .25      .50      .75      .90      .95
     135        0      133        1   0.8384  0.05065   0.7260   0.7551   0.8308   0.8539   0.8712   0.8817   0.8868

lowest : 0.6662404 0.6682187 0.6694510 0.6893836 0.6899561, highest: 0.8929477 0.8929531 0.8929544 0.8985774 0.9118788
```

23 pav. Transakcijų vertinimo koeficiento trečiajame klasteryje apžvalga

Ketvirtajame klasteryje yra 28 transakcijos. Šio klasterio vertinimo koeficientas yra aukščiausias iš visų. Vidurkis siekia net 0.91. Šiame klasteryje yra tik viena transakcija, kurios vertinimo koeficientas yra mažesnis nei 0.8.

```
Koeficientas
       n  missing distinct     Info     Mean      Gmd      .05      .10      .25      .50      .75      .90      .95
      28        0       27        1   0.9095  0.07116   0.8067   0.8147   0.8975   0.9153   0.9424   0.9977   1.0000

lowest : 0.7082942 0.8024733 0.8146821 0.8147161 0.8500567, highest: 0.9501236 0.9892230 0.9967612 0.9999187 1.0000000
```

24 pav. Transakcijų vertinimo koeficiento ketvirtajame klasteryje apžvalga

Rezultate matome, kad kiekvienas klasteris turi po kelias transakcijas, kurios turi žemesnį vertinimo koeficientą. Ketvirtasis klasteris surinko geriausius vertinimo koeficiento įvertinimus. Trečiasis klasteris yra surinkęs mažiausius įvertinimus.

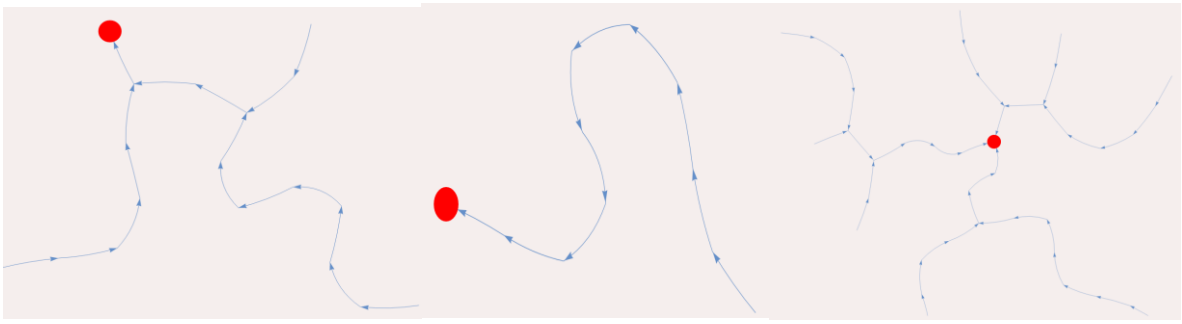
3.5. Transakcijų klasterių paaiškinimas

K-vidurkių klasteriai paskirsto transakcijų grafus į 4 skirtingus klasterius. Žemiau pateiktoje lentelėje (žr. 21 lentelėje) galima rasti klasterių sutrumpintą apibūdinimą.

22 lentelė. Sutrumpintas klasterių apibūdinimas

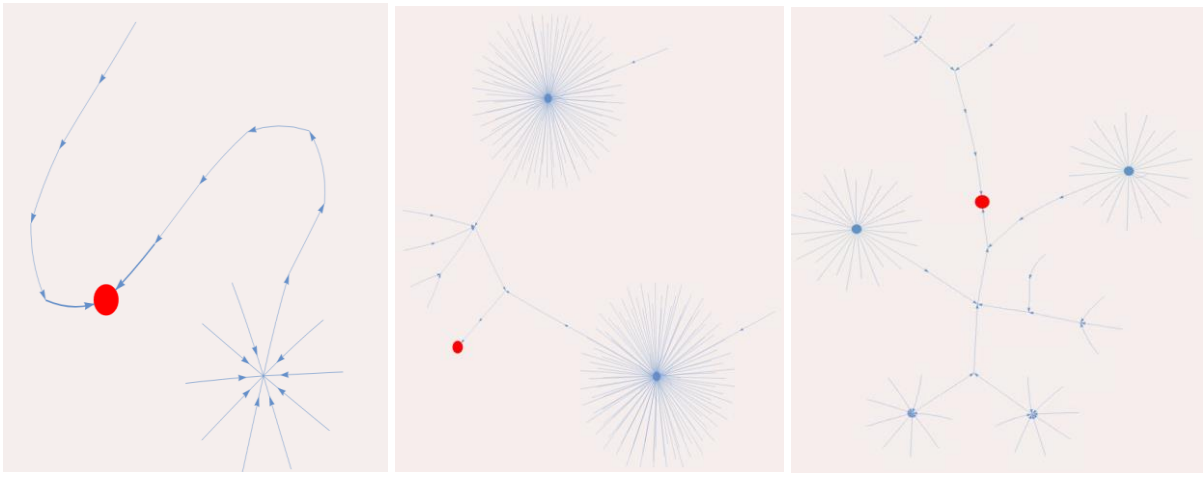
	1 klasteris (869 grafai)	2 klasteris (243 grafai)	3 klasteris (135 grafai)	4 klasteris (28 grafai)
Grafo viršūnės (vidurkis)	90	33 596	244 767	17
Aukščiausias grafo viršūnės laipsnis (vidurkis)	17	630	892	4.5
Vidutinis grafo viršūnės laipsnis	2	2.2	3.1	1.9
Vidutinis mokestis už transakciją	0.000036 BTC	0.0047	0.0026 BTC	0.00073 BTC
Vidutinis įvesčių skaičius	11	251	196	2.5
Vidutinis išvesčių skaičius	24	48	67	13
Vidutinė transakcijų vertė	30 BTC	5.4 BTC	1.6 BTC	13 BTC
Vidutinis transakcijų laiko skirtumas	6 054 min	5 560 min	1 341 min	341 098 min
Trumpiausias vidutinis laiko skirtumas tarp transakcijų minutėmis.	91 min	2.5 min	0.71 min	2 449 min
Transakcijų skaičius per dieną vidutiniškai	13	2 119	11 966	3.7
Vertinimo koeficiento vidurkis	0.8994	0.8517	0.8384	0.9095

1. Pirmasis klasteris turi didesnius transakcijų grafus, tačiau jie nėra sudėtingi, atliekamos transakcijos turi mažą išvesčių bei įvesčių skaičių, nėra atliekamos per greitai ar per dažnai. Šiame klasteryje vyrauja ganėtinai didelės transakcijų sumos, vidurkis siekia 30BTC. Transakcijų vertinimo koeficiento vidurkis lygus 0.8994. Didžioji dalis grafų yra sudaryti iš paprastos grandinės, transakcijos yra vykdomos turint vieną įvestį, nėra sudėtingų išsišakojimų. Tokių paprastos sandaros grafų šiame klasteryje yra net 58%. Paveikslėlyje (25 pav.) yra pavaizduoti paprastos sandaros grafai. Grafe pavaizduotas didesnis raudonas taškas žymi paskutinę transakciją, likusios viršūnės gali būti skirtingo dydžio priklausomai nuo įvesties sumos dydžio, jeigu didelė įvesties transakcijos suma, tuomet grafo viršūnė yra didesnė. Šiuo atveju sumos yra ganėtinai panašios bei reikšmingai nesiskiria, nes viršūnės yra panašaus dydžio. Transakcijų grafai yra nesudėtingi, įtartinų veiklų negalima įžvelgti. Panašu, kad šiame klasteryje 58% transakcijų yra visiškai įprastos ekonominės veiklos, kurios metu perkama ar atsiskaitoma už paslaugas ar prekes, pervedamos lėšos artimiesiems ar panašaus tipo veiklos. Šios transakcijos gali atspindėti visas ekonomines veiklos rūšis, kuriose naudojamos bitkoino monetos (žr. 2 lentelėje) dėl savo paprastos sandaros.



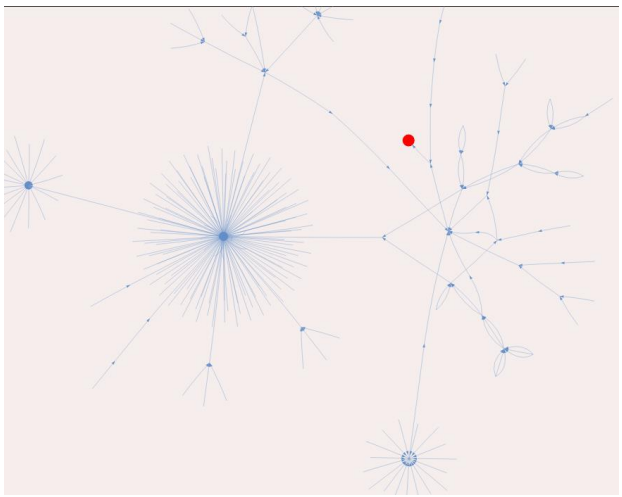
25 pav. Transakcijų grafai

Kita dalis klasterio transakcijų grafų yra nesudėtingi grafai, tačiau turintys daugiau nei kelias įvestis (26 pav.). Tokių transakcijų yra apie 35% visų klasterio transakcijų. Šie transakcijų grafai sudaryti iš įprastų nesudėtingų transakcijų, tačiau turi vieną ar kelias įvestis, kurios sudarytos iš daugiau nei 2 įvesčių. Jeigu transakcija yra sudaryta iš didelio skaičiaus įvesčių, tai nebūtinai gali reikšti, kad transakcija yra įtartina, tačiau tai gali būti viena iš galimybių. Gali būti, kad transakcija yra sudaryta iš kelių įvesčių todėl, kad siunčiant atitinkamą bitkoino monetą, reikėjo panaudoti smulkesnes, anksčiau gautas monetas.



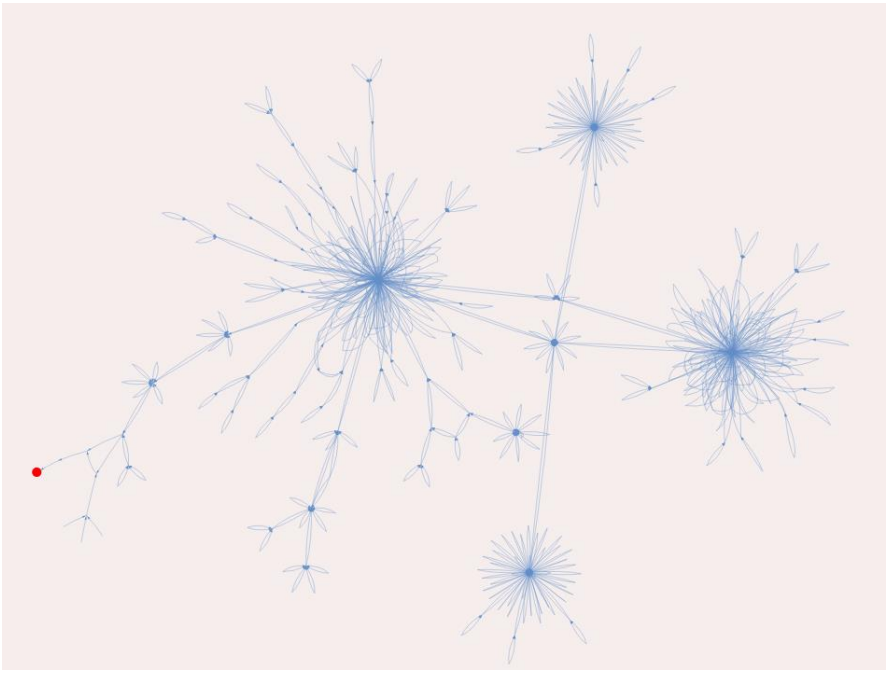
26 pav. Transakcijų grafai pirmame klasteryje

Pirmajame klasteryje taip pat yra priskirti grafai, kurie yra sudėtingesni. Paveikslėlyje (27 pav.) matosi, kad transakcijos sudarytos iš daugelio įvesčių, taip pat matome, kad yra transakcijos, kurių įvestys yra kilpinės, persipynusios tarpusavyje. Kilpinės transakcijos reiškia, kad buvo pateiktos dvi (ar daugiau) įvesčių transakcijai iš to pačio adreso, su skirtingomis sumomis. Taip atsitinka todėl, kad siuntėjas kas kartą siųsdamas lėšas gauna grąžą. Grąžą galima pasirinktinai gauti į savo piniginę arba į atskirą grąžos piniginę. Vėliau, turint keletą grąžų ir norint tas lėšas pervesti kitur, tos transakcijos naudojamos kaip įvesties transakcijos. Tokiu atveju susidaro kelios skirtingos įvesties transakcijos iš to pačio adreso, tačiau su skirtingomis sumomis. Transakcijos, kurios turi didelį kiekį įvesčių, gali būti suformuotos stengiantis sustambinti bitkoino monetą.



27 pav. Transakcijų grafas pirmame klasteryje

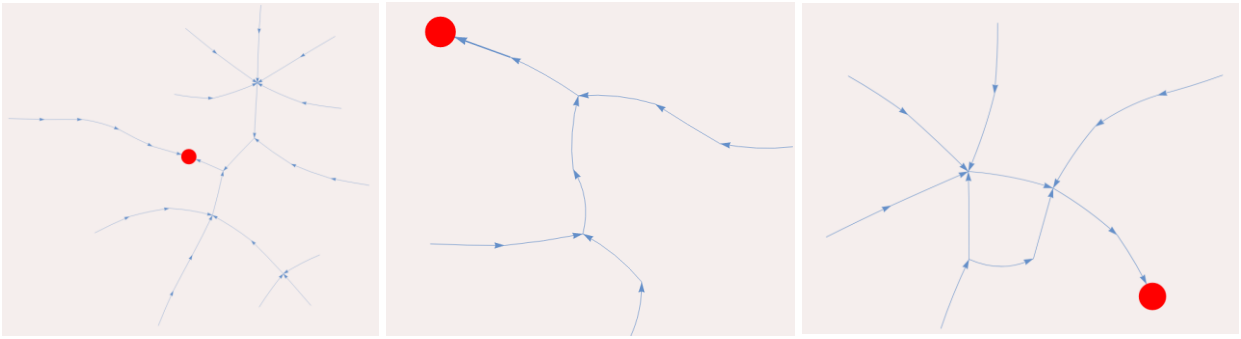
Šiame paveikslėlyje (28 pav.) matome, kad transakcijų grafas yra ypač sudėtingas, vyrauja transakcijos turinčios keletą įvesčių, kai kurios transakcijos turi netgi dešimtis įvesčių. Daug yra kilpinių transakcijų. Šis grafas atrodo daug įdomesnis todėl, kad yra daugybė kilpinių transakcijų. Taip pat transakcijų viršūnę žymintis taškas „gėlyčių“ centre yra didesnis, vadinasi, transakcijų suma yra didesnė. Panašu, kad tokio tipo transakcijos padeda sustambinti bitkoino monetą. Kadangi viršūnių dydis yra didesnis, vadinasi, transakcijose naudojamos didesnės lėšų sumos.



28 pav. Transakcijų grafas pirmame klasteryje

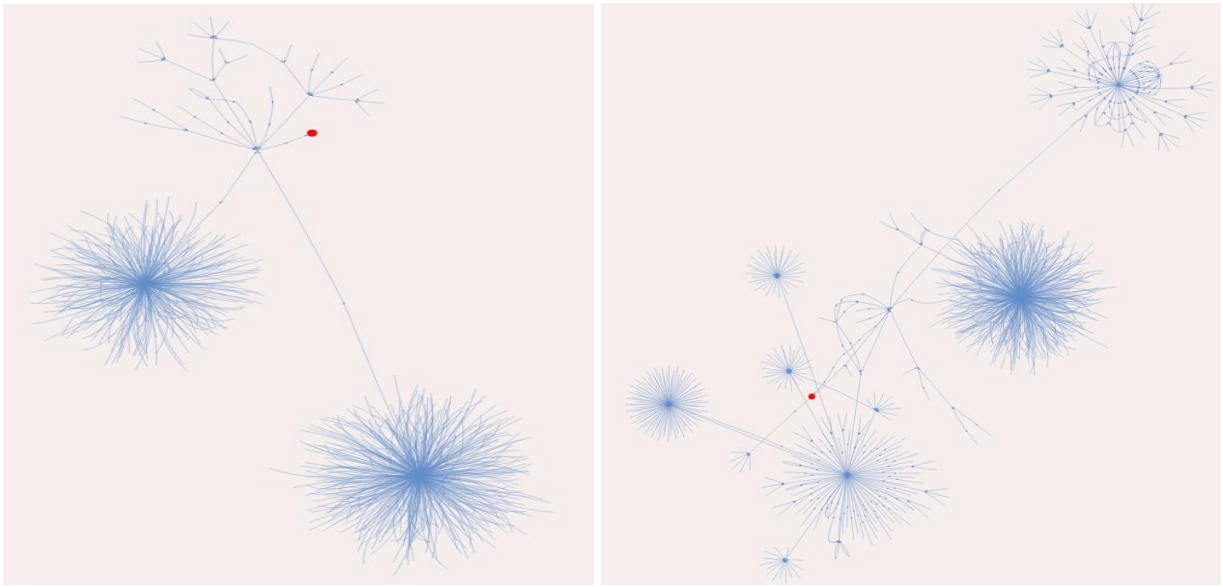
2. Ketvirtasis klasteris yra panašus į pirmąjį, transakcijų vertinimo koeficientas yra šiek tiek didesnis nei pirmojo klasterio. Taip pat šiame klasteryje yra išskirtas nedidelis skaičius transakcijų bei jų vidutinė vertė yra mažesnė, siekia 13BTC. Transakcijos atliekamos lėtai, vidutiniškai kas beveik 2 dienas ir yra įvykdomos tik keletas transakcijų per dieną. Didžiausias skirtumas tarp pirmojo ir ketvirtojo klasterių yra tai, kad ketvirtajame klasteryje

transakcijos atliekamos lėčiau bei yra šiek tiek mažesnės vertės. Dauguma transakcijų grafų ketvirtajame klasteryje yra paprasti, tiesiniai, sudaryti iš vienos įvesties (29 pav.). Ketvirtajame klasteryje yra vykdomos įprastos finansinės operacijos. Bitkoinai pervedami lėtai, iš vienos sąskaitos į kitą, bitkoino monetos turi mažesnę įvesčių istoriją.



29 pav. Transakcijų grafai ketvirtajame klasteryje

3. Antrajame klasteryje vyrauja dideli transakcijų grafai. Šiame klasteryje transakcijos atliekamos greitai, vidutiniškai kas 2.5 min., yra atliekamos apie 2 119 transakcijos per dieną. Šis klasteris turi žemesnį vertinimo koeficientą, kuris siekia 0.8517, vadinasi, transakcijos yra sudėtingesnės, greitesnės, yra mokamas didesnis transakcijos įvykdymo mokestis. Didesnis transakcijos įvykdymo mokestis yra mokamas tuomet, kai transakcija yra sudėtinga arba kai norima transakciją patvirtinti kaip įmanoma greičiau. Matome paveikslėlyje (30 pav.), kad kelios transakcijų grafo viršūnės turi ypatingai didelį įvesčių skaičių.



30 pav. Transakcijų grafai antrajame klasteryje

4. Trečiojo klasterio vertinimo koeficientas yra žemiausias – 0.8384. Šiame klasteryje priskirti transakcijų grafai, kuriuose transakcijos įvykdomos greičiausiai, trumpiausias laikas tarp transakcijų nesiekia net minutės, o pervedamos sumos vidutinė vertė klasteryje lygi 1.6 BTC bei transakcijų grafai yra sudėtingiausi. Šiame klasteryje atliekamos vidutiniškai beveik 12 000 transakcijų per dieną. Tai ypač didelis skaičius todėl, kad transakcijos atliekamos labai greitai, transakciją sudaro daug įvesčių, tas įvestis sudaro dar daugiau įvesčių ir visos jos

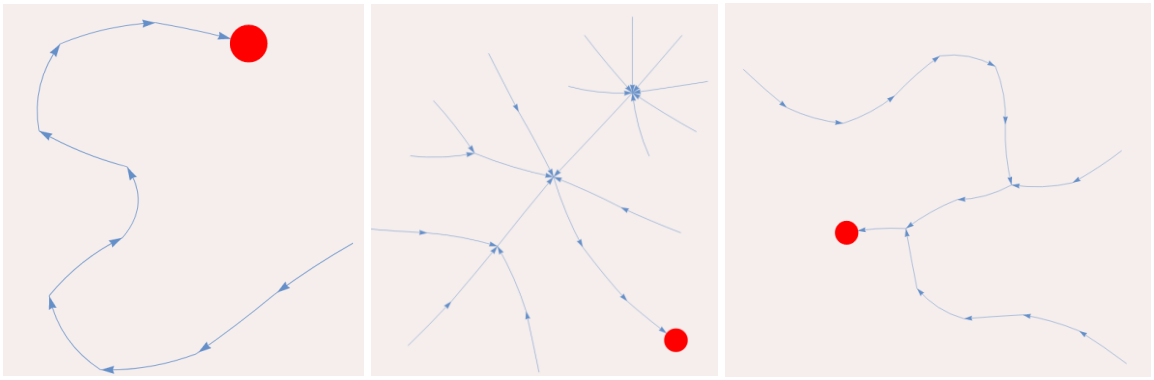
vykdomos ganėtinai greitai. Šis klasteris yra vienas iš sudėtingiausių ir yra labiausiai įtartinas lyginant su kitais. Taip yra todėl, kad viena iš pagrindinių sumaišymo tinklalapių idėjų ir yra vykdyti skirtingo dydžio, nedideles transakcijas iš skirtingų piniginių, maišyti bei permaišyti bitkoino monetas bei tai atlikti ganėtinai greitai, siekiant gauti kitas sumaišytas bitkoino monetas, kurios turi kur kas keblesnę istoriją ir ją sunkiau atsekti. Visi transakcijų grafai šiame klasteryje turi daugiau nei 72 256 viršūnes, todėl tokius grafus yra sudėtinga pavaizduoti grafiškai. Didžiausi transakcijų grafai turi virš 500 000 viršūnių. Žinant, kad šiame tyrime yra analizuojami transakcijų grafai, kurie sudaryti iš 10 žingsnių transakcijų istorijos, galima teigti, kad 500 000 viršūnių yra labai daug bei tokios transakcijos yra ypatingai sudėtingos. Galima daryti prielaida, kad tokie grafai turi daug daugiau viršūnių, jeigu analizėje nebūtų apribotas transakcijų žingsnių atgal skaičius. Tokio tipo transakcijos kelia didžiausią įtarimą bei šis klasteris turėtų būti peržvelgiamas atidžiau, siekiant išsiaiškinti, ar esamos transakcijos nėra susijusios su nelegaliomis veiklomis, ar transakcijos nėra susijusios tarpusavyje.

3.6. Transakcijų klasterių priskyrimas ekonominėms veiklos rūšims

Transakcijos yra įvykdomos dėl tam tikrų priežasčių, todėl visi gauti klasteriai atspindi tam tikras ekonomines veiklas. Pagal transakcijų grafą galima daryti prielaidas, kokio tipo ekonominės veiklos rūšis tai būtų.

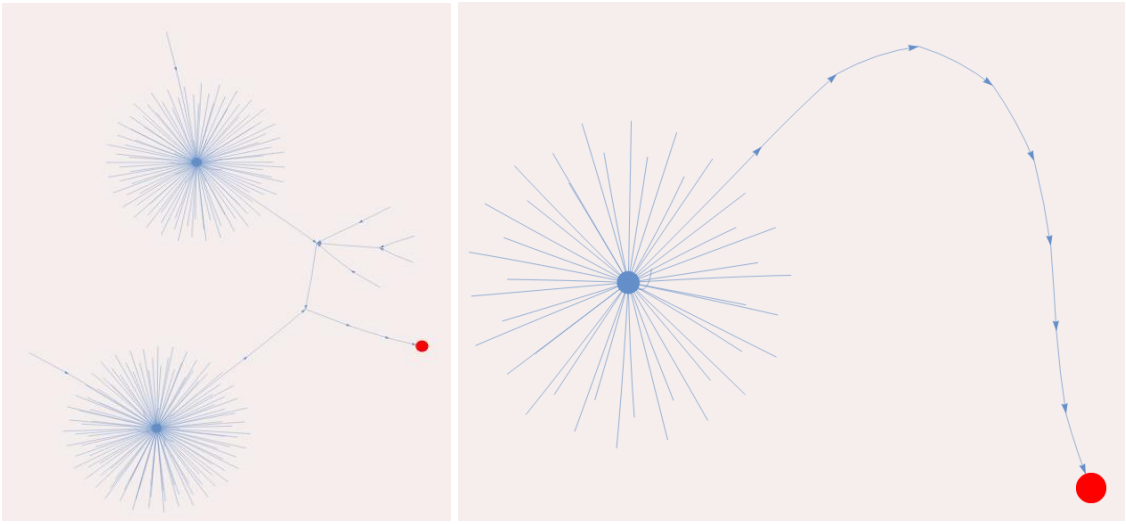
Anksčiau minėtoje ekonominių veiklų apžvalgoje aptariamos ekonominės veiklos rūšys pagal sektorių, kuriose yra naudojamas bitkoinas. Taigi atsiskaitymai bitkoino monetomis yra būdingi: statybai, didmeninei ir mažmeniniai prekybai, viešbučių bei restoranų veikloje, transporto ar sandėliavimo veikloje, finansiniame tarpininkavime, nekilnojamame turte, švietime bei meninėje ar pramoginėje veikloje.

1. Pirmasis klasteris yra didžiausias bei jame yra nesudėtingų grafų struktūrų transakcijos. Didžioji dalis klasterių yra sudaryta iš paprastos sandaros grafų (31 pav.). Tokie grafai sudaro 58% visų pirmojo klasterio transakcijų. Tokios struktūros grafai atspindi įprastas ekonomines veiklas, kurių metu yra perkama ar atsiskaitoma už paslaugas ar prekes pervedamos lėšos artimiesiems ar panašaus tipo veiklos. Šios transakcijos gali atspindėti visas ekonomines veiklos rūšis, kuriose naudojamos bitkoino monetos. Dažniausiai tokio tipo transakcijų grafai vaizduoja sekcijos G ekonomines veiklas – didmeninė bei mažmeninė prekyba. Taip pat gali būti ir kitos ekonominės veiklos, kurių metu vykdomi įprasti, nesudėtingi atsiskaitymai.



31 pav. Pirmojo klasterio grafai

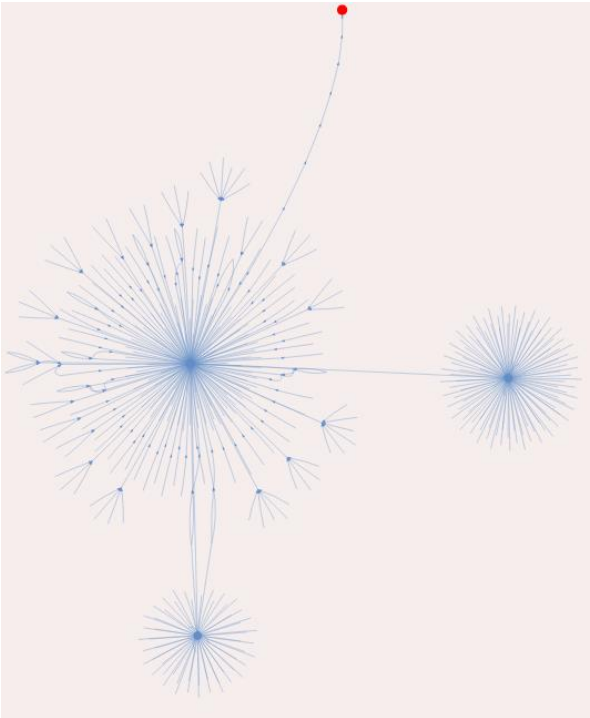
Šiame klasteryje taip pat yra sudėtingesnės sandaro grafų, kurie vis dar nėra labai sudėtingi, tačiau turi transakcijas, kuriose yra kelios įvestys (32 pav.). Šiuo atveju galima būtų atpažinti didmeninės ar mažmeninės prekybos veiklas, kurio metu gali būti pervedamos lėšos iš kelių piniginių į vieną, siekiant nusipirkti didesnę prekę ar brangesnę paslaugą. Taip pat galima įžvelgti statybos ar ekonominių veiklų susijusių su nekilnojamuoju turtu, todėl kad nekilnojamo turto kainos yra didesnės, todėl gali būti, kad reikalingos didesnės lėšos norint nusiųsti didesnę sumą pardavėjams. Galimai didesnis įvesčių skaičius rodo kelis žmones prisidėjusius prie pirkinio arba vienas asmuo turėjo kelias skirtingas pinigines ir nori naudoti jų lėšas kartu. Dar sektoriaus H ekonominės veiklos susijusios su viešbučiais ir restoranais gali paaiškinti tokio tipo transakcijų grafus. Viešbučiai bei restoranai gauna lėšas iš daugelio klientų, tuomet norėdami tas lėšas panaudoti jie transakcijoje turės ne vieną įvestį, nes lėšos yra atkeliavusios iš skirtingų piniginių, skirtingų klientų. Panašu, kad tokio tipo transakcijų grafai atspindi ekonomines veiklas, kuriose keli pirkėjai moka už prekes ar paslaugas bei perveda lėšas į vieną piniginę, o tuomet lėšos yra pervedamos kitur.



32 pav. Pirmojo klasterio sudėtingesni grafai

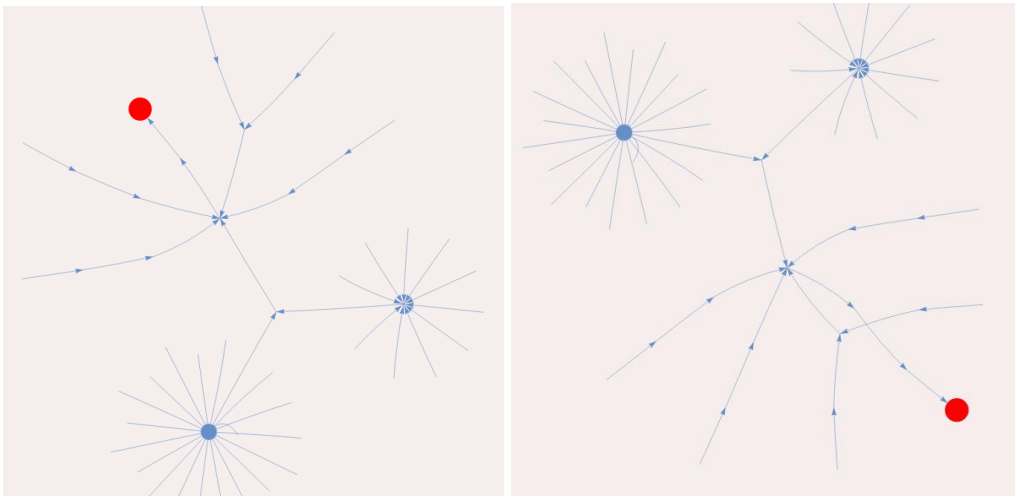
Sudėtingiausi transakcijų grafai pirmame klasteryje turi daugelį įvesčių (33 pav.). Šiuo atveju tai gali būti statyba, didmeninė ar mažmeninė prekyba, viešbučiai bei restoranai, gali būti ir finansinio tarpininkavimo ekonominės veiklos. Labai daug matome kilpinių transakcijų, vadinasi, bitkoino monetos yra stambinamos, siunčiamos transakcijos yra didesnių sumų. Tokios veiklos dažniausiai atspindi viešbučius, nekilnojamo turto

pardavimus ar nekilnojamo turto statybas. Tokio tipo transakcijos taip pat gali būti susijusios su sekcijos R veiklomis – meninės, pramogų ir poilsio veiklos. Šiuo atveju gali būti, kad lėšos buvo pervedamos iš daugelio piniginių siekiant susimokėti už tam tikrą pramogą. Tuomet norima lėšas sustambinti į didesnę bitkoino monetą, todėl transakcija turi daugelį įvesčių.



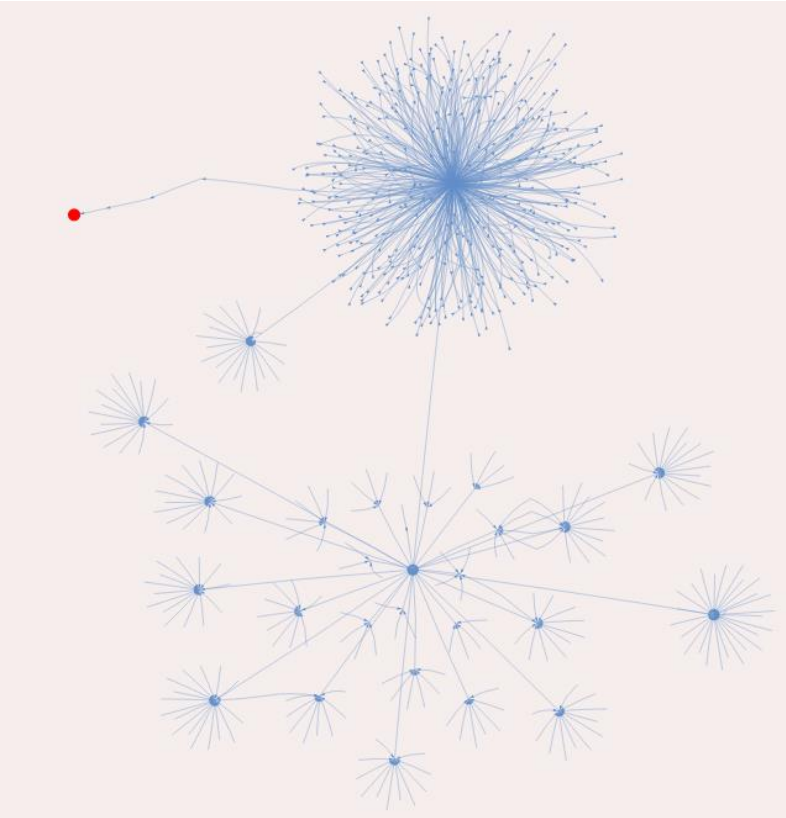
33 pav. Pirmojo klasterio sudėtingiausias grafas

2. Ketvirtajame klasteryje situacija yra panaši kaip ir pirmajame. Klasteriai yra nesudėtingi, tačiau turi didesnį skaičių įvesčių (34 pav.). Galima daryti prielaidą, kad šiame klasteryje yra vykdoma įprasta prekių pirkimo ar paslaugų įsigijimo veikla. Taip pat gali būti vykdomos švietimo ekonominės veiklos, kurios metu mokama studijų įmoka, ar perkamos švietimo paslaugos. Tokios paslaugos yra atliekamos lėtai bei nedidelėmis sumomis lyginant su nekilnojamu turtu. Tokio tipo transakcijos gali atspindėti įprastą prekybos ir paslaugų veiklą, kadangi naudojamas nedidelis kiekis įvesčių transakcijų, galima mažesnės monetos yra stambinamos į didesnę sumą.



34 pav. Ketvirtojo klasterio grafai

3. Antrajame klasteryje yra dideli transakcijų grafai. Tokio tipo transakcijas galima priskirti ekonominei veiklai sektoriuje R – meninė, pramoginė ar poilsio veikla, susijusi su lažybomis, aukcionu ar lėšų aukojimu. Gali būti lažybų turnyrų tipo transakcija, kurios metu dalyviai perveda tam tikrą lėšų sumą į vieną piniginę, o po įvykusio renginio, nugalėtojas arba keli nugalėtojai gauna piniginį apdovanojimą. Taip pat tokio tipo transakcijos gali būti pervedamos į bitkoinų keityklas. Norint išgryninti bitkoinų monetas į įprastą piniginę valiutą, reikia naudotis bitkoinų keityklomis. Tuomet lėšos yra pervedamos į vieną iš keityklų piniginę. Tai galėtų būti sektoriaus J ekonominės veiklos, susijusios su finansiniu tarpininkavimu. Šis grafas turi daugelį įvesčių ir dažniausiai viena išvestį. Šiuo atveju galėtų būti lažybų, pokerio, kazino veiklų tipo transakcija.



35 pav. Antrojo klasterio transakcijos grafas

4. Trečiasis klasteris yra sudarytas iš didžiausių transakcijų grafų. Šie grafai turi daugiau nei puse milijono viršūnių, todėl grafiškai aiškiai ir suprantamai pavaizduoti yra sudėtinga. Panašu, kad šiame klasteryje yra vaizduojamos sektoriaus J ekonominės veiklos, kurios susijusios su finansiniu tarpininkavimu. Yra ne viena finansines paslaugas teikianti interneto svetainė, kuri padeda sustambinti bitkoino monetas bei tokiu būdu suteikti „švarias“ monetas savininkui. Šios ekonominės veiklos taip pat gali būti priskiriamos sukčiavimo atvejams. Toks monetų stambinimas ir smulkinamas yra neretai atliekamas tamsiajame internete, kuomet asmenys nori paslėpti tikrąją monetų prigimtį. Kita galima ekonominė veikla yra susijusi su prekyba. Internetinės prekybos atveju gali būti atliekamos transakcijos labai greitai bei įvairių sumų. Šiuo atveju šie transakcijų grafai galėtų vaizduoti aktyvią prekybą bei greitą lėšų pervedimą. Tiesa, šis klasteris yra vienas įdomiausių, kadangi transakcijų grafai yra sudėtingi, komplikuoti bei neatspindi tipiškų ekonominių veiklų. Šis klasteris gali būti nagrinėjamas atidžiau bei galimai būtų atrasti sukčiavimo atvejai.

3.7. Tyrimo rezultatų aptarimas

Atliktas tyrimas parodė, kad 700 000 bloke galima išskirti 4 skirtingus klasterius. Du iš šių klasterių galima būtų apjungti į vieną grupę, kiti du klasteriai apjungė transakcijų grafus, kurie yra labiau sudėtingesni. Antrasis bei trečiasis klasteriai išskyrė transakcijas, kurios yra sudėtingos, turinčios didelį skaičių įvesčių bei išvesčių bei atliekamos labai greitai. Sudėtingiausias klasteris yra trečiasis. Šiame klasteryje transakcijų grafai yra labai dideli bei sudėtingi, transakcijos turi didelį skaičių įvesčių bei išvesčių, transakcijos atliekamos greitai, todėl transakcijos tampa įtartinos, nes sunku priskirti transakcijų grafus įprastai ekonominei veiklai.

Transakcijų vertinimo koeficientas suskirstė transakcijas į panašius klasterius kaip k-vidurkių metodas. Galima daryti prielaidą, kad transakcijų vertinimo koeficientas padeda įvertinti pavienes transakcijas, transakcijų grafus bei nustatyti ar transakcijos yra vertos gilesnės analizės. Šio tyrimo rezultatai rodo, kad įvestų parametrų užtenka norint atskirti įtartinas transakcijas, tačiau galima įtraukti daugiau parametrų, siekiant išskirti ypač sudėtingas transakcijas bei sumažinti įtartinų transakcijų skaičių. Žinant įtartinų, su nelegalia veikla susijusių virtualių piniginių adresus, galima būtų vertinti transakciją atitinkamai. Jeigu transakcija yra atliekama tam pačiam adresui keletą kartų, tačiau skirtingu laiko momentu, tai taip pat galėtų būti įvertinta. Taigi transakcijų vertinimo koeficientas gali būti papildytas papildomais parametrais.

Išvados

1. Atlikus literatūros analizę, matome, kad bitkoino naudojimas finansinėse veiklose yra gana plačiai paplitęs. Dėl bitkoino blokų grandinės savybių, ypač pseudo anonimiškumo, bitkoinas neretai yra naudojamas pinigų plovimo schemose. Yra skirtingų pinigų plovimo schemų arba bitkoino monetų „švarinimo“ būdų, kurie yra plačiai paplitę juodajame internete. Atlikti tyrimai parodė, kad įtartinas veiklas galima identifikuoti tiriant transakcijas bei pritaikant matematinius modelius. Analizuojant kitų autorių atliktus tyrimus pastebėta, kad dauguma jų analizuoja transakciją bei jos parametrus. Keli autoriai tyrė transakcijų grafus, tačiau grafų skaičius buvo nedidelis bei duomenų rinkinys buvo pateiktas išorinės įmonės, kuri pateikė jau atpažintų įtartinų transakcijų grafus, todėl buvo pritaikyti mašininiai mokymai norint identifikuoti panašias įtartinas transakcijas.
2. Norint atsekti įtartinas bitkoino transakcijas, naudinga tirti ne tik pačią bitkoino transakciją ir jos parametrus, tačiau ir buvusias transakcijas. Ypač populiarūs bitkoino monetų „sumaišymo“ platformos vykdo didelį skaičių transakcijų, kuriose smulkina bei stambina bitkoino monetas. Transakcijų grafai padeda identifikuoti tokio tipo veiklas bei taip pat padeda priskirti transakcijas galimoms ekonominėms veikloms.
3. Bitkoino transakcijų grafai yra puikus įrankis įtartinų veiklų bitkoino blokų grandinėje atpažinimui. Bitkoino transakcijų grafai yra skirtingo sudėtingumo ir skirtingų parametrų. Vieni grafai atskleidžia įprastą ekonominę veiklą, kiti grafai yra sudėtingesni bei reikalauja gilesnės analizės. Tyrimas parodė, kad dešimties transakcijų grafo žingsnių užtenka pamatyti įtartiną transakcijų grafo struktūrą. Tiriant 10 žingsnių transakcijų grafus galima palyginti ir kitus parametrus tarpusavyje – įvesčių, išvesčių skaičių, transakcijos mokesčio dydį bei transakcijos laiką. Jeigu yra pakankamai geri kompiuteriniai resursai, tuomet galima analizuoti didesnius transakcijų grafus, tokiu būdu išplečiant transakcijų grafo žingsnių skaičių.
4. Atlikus įvairius transakcijų grafų klasterizavimo metodus, pastebėta, kad geriausiai tinka k-vidurkių metodas. Šis metodas geriausiai išskyrė panašias transakcijų grafų grupes. Labiausiai netinkamas yra tankiu grįstas klasterizavimas. Transakcijų vertinimo koeficientas yra tinkamas įrankis norint įvertinti kiekvieną iš grafo transakcijų atskirai. Tokiu būdu galima matyti kiek grafe yra įprastų transakcijų bei kiek grafe yra sudėtingų ar greitų transakcijų, kuomet transakcijų vertinimo koeficientas mažėja. Esant geresniems kompiuteriniams resursams bei turint daugiau transakcijos parametrų, galima papildyti transakcijų vertinimo koeficientą papildomomis taisyklėmis. Tokiu būdu įtartinų transakcijų sąrašas būtų susiaurintas. Tyrimo rezultatuose matome, kad vertinimo koeficientas įvertino transakcijas taip pat kaip k-vidurkių klasterizavimo metodas. Galima daryti išvadas, kad vertinimo koeficientas yra efektyvus būdas įvertinti transakcijas. Šio vertinimo koeficiento privalumai yra tie, kad galima paskaičiuoti vertinimo koeficiento įvertį vienos transakcijos grafui. Tokiu būdu galima gauti įvertį, kuris parodo ar transakcija yra įtartina ar ne.
5. Atlikus tyrimą, matome, kad transakcijų grafai atspindi tam tikras ekonomines veiklas. Vyrauja įprastos ekonominės veiklos, kurių metu yra perkamos ar parduodamos paslaugos ar prekės, vykdoma statybų ar su nekilnojamu turtu susijusi veikla, finansinis tarpininkavimas. Tyrimo metu yra išskirtas klasteris, kurio veiklą yra sudėtingiausia pagrįsti ekonomine veiklos rūšimi dėl didelio transakcijų skaičiaus bei transakcijų vykdymo dažnumo ir greitumo. Norint išplėsti tyrimo rezultatus, galima įtraukti daugiau parametrų apie transakcijas. Įtraukus transakcijų

gavėjo piniginės adresą, galima būtų asocijuoti tam tikras pinigines su įtartinomis transakcijomis.

Literatūros sąrašas

1. ZHENG, Baokun, et al. Malicious bitcoin transaction tracing using incidence relation clustering. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* [interaktyvus]. 2018, 313–323 [žiūrėta 2023-05-15]. DOI 10.1007/978-3-319-90775-8_25. Prieiga per: https://eudl.eu/pdf/10.1007/978-3-319-90775-8_25
2. LORENZ, Joana, et al. Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity. *Proceedings of the First ACM International Conference on AI in Finance* [interaktyvus]. 2020 [žiūrėta 2023-05-15]. DOI 10.1145/3383455.3422549. Prieiga per: https://arxiv.org/abs/2005.14635
3. NAKAMOTO, Satoshi. *Bitcoin: A peer-to-peer electronic cash system* [interaktyvus]. 2008. [žiūrėta 2023-05-15]. Prieiga per: https://bitcoin.org/bitcoin.pdf?satoshi=nakamoto
4. GARRATT, Rodney and WALLACE, Neil, 2018, Bitcoin 1, Bitcoin 2, ...: An experiment in privately issued outside monies. *Economic Inquiry* [interaktyvus]. 2018, 56(3), 1887–1897 [žiūrėta 2023-05-15]. DOI 10.1111/ecin.12569. Prieiga per: https://onlinelibrary.wiley.com/doi/full/10.1111/ecin.12569
5. SHAHZAD, Syed Jawad, et al. Is bitcoin a better safe-haven investment than gold and commodities? *International Review of Financial Analysis* [interaktyvus]. 2019, 63,322–330 [žiūrėta 2023-05-15]. DOI 10.1016/j.irfa.2019.01.002. Prieiga per: https://www.sciencedirect.com/science/article/pii/S1057521918306604
6. MARTHINSEN, John E. and GORDON, Steven R., 2022, The price and cost of Bitcoin. *The Quarterly Review of Economics and Finance* [interaktyvus]. 2022, 85, 280–288 [žiūrėta 2023-05-15]. DOI 10.1016/j.qref.2022.04.003. Prieiga per: https://arxiv.org/abs/2204.13102
7. VRANKEN, Harald. Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability* [interaktyvus]. 2017, **28**, 1–9 [žiūrėta 2023-05-15]. ISSN 1877-3435. doi:10.1016/j.cosust.2017.04.011
8. CHOHAN, Usman W. A History of Bitcoin. *SSRN Electronic Journal* [interaktyvus]. 2017 [žiūrėta 2023-05-15]. ISSN 1556-5068. doi:10.2139/ssrn.3047875
9. WU, Yan, et al. A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation. *IEEE Transactions on Network Science and Engineering* [interaktyvus]. 2020, 1 [žiūrėta 2023-05-15]. ISSN 2334-329X. doi:10.1109/tnse.2020.2970113
10. WU, Yan, et al. A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation. *IEEE Transactions on Network Science and Engineering* [interaktyvus]. 2020, 1 [žiūrėta 2023-05-15]. ISSN 2334-329X. Prieiga per: doi:10.1109/tnse.2020.2970113
11. COINTELEGRAPH. What is the Bitcoin blockchain? A guide to the technology behind BTC. *Cointelegraph* [interaktyvus]. 14 March 2022 [žiūrėta 2023-05-15]. Prieiga per: https://cointelegraph.com/learn/how-does-blockchain-work-a-beginners-guide-to-blockchain-technology
12. SHAHZAD, Syed Jawad Hussain, et al. Is Bitcoin a better safe-haven investment than gold and commodities? *International Review of Financial Analysis* [interaktyvus]. 2019, **63**, 322–330 [žiūrėta 2023-05-15]. ISSN 1057-5219. Prieiga per: doi:10.1016/j.irfa.2019.01.002

13. ZHANG, Yu-Dong. A Survey of Blockchain Security Issues and Challenges. *International Journal of Neural Systems* [interaktyvus]. 2021, **31**(06), 2103006 [žiūrėta 2023-05-15]. ISSN 1793-6462. Prieiga per: doi:10.1142/s0129065721030064
14. WAGSTAFF, Jeremy. Mt. Gox bitcoin debacle: huge heist or sloppy glitch? *U.S.* [interaktyvus]. 2014 [žiūrėta 2023-05-15]. Prieiga per: https://www.reuters.com/article/bitcoin-mtgox-heist-idUSL3N0LX2SP20140228
15. IRWIN, Angela S. M., and Adam B. TURNER. Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of Money Laundering Control* [interaktyvus]. 2018, **21**(3), 297–313 [žiūrėta 2023-05-15]. ISSN 1368-5201. Prieiga per: doi:10.1108/jmlc-07-2017-0031
16. Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report. *Ciphertrace* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/
17. Gaihre, Anil et al. "Do Bitcoin Users Really Care About Anonymity? An Analysis of the Bitcoin Transaction Graph." *2018 IEEE International Conference on Big Data (Big Data)* [interaktyvus]. 2018, 1198-1207 [žiūrėta 2023-05-15]. Prieiga per: https://www.semanticscholar.org/paper/Do-Bitcoin-Users-Really-Care-About-Anonymity-An-of-Gaihre-Luo/e6b3a7c8de07bd183b7f02c9ff2fa1d9a099f15b
18. MEIKLEJOHN, Sarah, et al. A fistful of bitcoins. In: *IMC'13: Internet Measurement Conference* [interaktyvus]. New York, NY, USA: ACM, 2013 [žiūrėta 2023-05-15]. ISBN 9781450319539. Prieiga per: doi:10.1145/2504730.2504747
19. REID, Fergal, et al. An analysis of anonymity in the bitcoin system. *In Security and privacy in social networks. Springer* [interaktyvus]. 2013, 197–223 [žiūrėta 2023-05-15]. Prieiga per: https://arxiv.org/abs/1107.4524
20. HARLEV, Mikkel Alexander, et al. Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning. In: *Hawaii International Conference on System Sciences* [interaktyvus]. Hawaii International Conference on System Sciences, 2018 [žiūrėta 2023-05-15]. ISBN 9780998133119. Prieiga per: doi:10.24251/hicss.2018.443
21. CHAINANALYSIS. The 2020 state of crypto crime. *Chainanalysis* [interaktyvus]. 2020 Prieiga per: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf
22. MOORE, Tyler; HAN, Jie; CLAYTON, Richard. The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs. In: I*nternational Conference on financial cryptography and data security. Springer*. Berlin, Heidelberg, 2012. p. 41-56.
23. WOLFSON, Shael N. Bitcoin: The Early Market. *Journal of Business & Economics Research (JBER)* [interaktyvus]. 2015, **13**(4), 201 [žiūrėta 2023-05-15]. ISSN 2157-8893. Prieiga per: doi:10.19030/jber.v13i4.9452
24. ULLAH, Subhan, et al. Assessing the influence of celebrity and government endorsements on bitcoin's price volatility. *Journal of Business Research* [interaktyvus]. 2022, **145**, 228–239 [žiūrėta 2023-05-15]. ISSN 0148-2963. Prieiga per: doi:10.1016/j.jbusres.2022.01.055
25. PIÑEIRO-CHOUSA, Juan, et al. Does social network sentiment influence the relationship between the S&P 500 and gold returns? *International Review of Financial*

Analysis [interaktyvus]. 2018, **57**, 57–64 [žiūrėta 2023-05-15]. ISSN 1057-5219. Prieiga per: doi:10.1016/j.irfa.2018.02.005

26. SHEN, Dehua, Andrew URQUHART, and Pengfei WANG. Does twitter predict Bitcoin? *Economics Letters* [interaktyvus]. 2019, **174**, 118–122 [žiūrėta 2023-05-15]. ISSN 0165-1765. Prieiga per: doi:10.1016/j.econlet.2018.11.007
27. BAUR, Dirk G., and Lai HOANG. The Bitcoin gold correlation puzzle. *Journal of Behavioral and Experimental Finance* [interaktyvus]. 2021, **32**, 100561 [žiūrėta 2023-05-15]. ISSN 2214-6350. Prieiga per: doi:10.1016/j.jbef.2021.100561
28. List of Crypto Exchange Hacks: Updated For 2023 | HedgewithCrypto. *HedgewithCrypto* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/
29. COTTEN, Tim. Bitcoin Money Laundering and Mueller's 12. *Medium* [interaktyvus]. 19 July 2018 [žiūrėta 2023-05-15]. Prieiga per: https://blog.cotten.io/bitcoin-money-laundering-and-muellers-12-e2fa91097e12
30. TURNER, Adam Brian, Stephen MCCOMBIE, and Allon J. UHLMANN. Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science* [interaktyvus]. 2020, **2** [žiūrėta 2023-05-15]. ISSN 2624-9898. Prieiga per: doi:10.3389/fcomp.2020.600596
31. WU, Yan, et al. A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation. *IEEE Transactions on Network Science and Engineering* [interaktyvus]. 2020, 1 [žiūrėta 2023-05-15]. ISSN 2334-329X. Prieiga per: doi:10.1109/tnse.2020.2970113
32. LORENZ, Joana, et al. Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity. In: *ICAIF '20: ACM International Conference on AI in Finance* [interaktyvus]. New York, NY, USA: ACM, 2020 [žiūrėta 2023-05-15]. Prieiga per: doi:10.1145/3383455.3422549
33. CONTRIBUTORS TO WIKIMEDIA PROJECTS. History of bitcoin - Wikipedia. *Wikipedia, the free encyclopedia* [interaktyvus]. 2 November 2013 [žiūrėta 2023-05-15]. Prieiga per: https://en.wikipedia.org/wiki/History_of_bitcoin
34. China bans banks from bitcoin transactions. *The Sydney Morning Herald* [interaktyvus]. 5 December 2013 [žiūrėta 2023-05-15]. Prieiga per: https://www.smh.com.au/business/markets/china-bans-banks-from-bitcoin-transactions-20131206-2yugy.html
35. Users Bitcoins Seized by DEA. *Lets Talk Bitcoin* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://web.archive.org/web/20131009062454/http:/letstalkbitcoin.com/users-bitcoins-seized-by-dea/
36. CUTHBERTSON, Anthony. Bitcoin now accepted by 100,000 merchants worldwide. *International Business Times UK* [interaktyvus]. 4 February 2015 [žiūrėta 2023-05-15]. Prieiga per: https://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613
37. MAK Vienna Becomes First Museum to Use Bitcoin to Acquire Art, a Harm van den Dorpel. *ARTnews.com* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.artnews.com/art-news/market/mak-vienna-becomes-first-museum-to-acquire-art-using-bitcoin-a-harm-van-den-dorpel-3995/

38. Shirriff, Ken. Proposal for addition of bitcoin sign. *Unicode* [interaktyvus]. 2015 [žiūrėta 2023-05-15]. Prieiga per: https://www.unicode.org/L2/L2015/15229-bitcoin-sign.pdf
39. LUDWIG, Sean. Y Combinator-backed Coinbase now selling over $1M Bitcoins per month. *VentureBeat* [interaktyvus]. 8 February 2013 [žiūrėta 2023-05-15]. Prieiga per: https://venturebeat.com/business/coinbase-bitcoin/
40. WARREN, Tom. Microsoft now accepts Bitcoin to buy Xbox games and Windows apps. *The Verge* [interaktyvus]. 11 December 2014 [žiūrėta 2023-05-15]. Prieiga per: https://www.theverge.com/2014/12/11/7375771/microsoft-supports-bitcoin-payments
41. Japan OKs recognizing virtual currencies as similar to real money. *The Japan Times* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.japantimes.co.jp/news/2016/03/04/business/tech/japan-oks-recognizing-virtual-currencies-similar-real-money/#.WGnhBvHythE
42. Theft And Mayhem In The Bitcoin World. *Forbes* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://web.archive.org/web/20160807023213/http:/www.forbes.com/sites/francescoppola/2016/08/06/theft-and-mayhem-in-the-bitcoin-world/#3adc93c251ae
43. CONTRIBUTORS TO WIKIMEDIA PROJECTS. Ledger (journal) - Wikipedia. *Wikipedia, the free encyclopedia* [interaktyvus]. 16 September 2015 [žiūrėta 2023-05-15]. Prieiga per: https://en.wikipedia.org/wiki/Ledger_(journal)
44. KHARPAL, Arjun. Bitcoin value rises over $1 billion as Japan, Russia move to legitimize cryptocurrency. *CNBC* [interaktyvus]. 12 April 2017 [žiūrėta 2023-05-15]. Prieiga per: https://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html
45. MAULDIN ECONOMICS. Here's why Russia is opening the door to cryptocurrencies. *Business Insider* [interaktyvus]. 3 May 2017 [žiūrėta 2023-05-15]. Prieiga per: https://www.businessinsider.com/why-russia-legalized-cryptocurrencies-2017-5
46. Bitcoin is plunging, fast. Here's why. *The Independent* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.independent.co.uk/tech/bitcoin-latest-price-value-south-korea-regulation-a8173506.html
47. Bitcoin Price Chart and Tables | Finance Reference. *U.S. Inflation Calculator: 1635→2023, Department of Labor data* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.in2013dollars.com/bitcoin-price
48. IRRERA, Anna. PayPal to allow cryptocurrency buying, selling and shopping on its network. *U.S.* [interaktyvus]. 21 October 2020 [žiūrėta 2023-05-15]. Prieiga per: https://www.reuters.com/article/paypal-cryptocurrency-idINL1N2HB14UTax payment with cryptocurrencies — Kanton Zug (zg.ch)
49. LEVISOHN, Ben. Bitcoin Is Crashing. Where It Might Be Headed Next. *Barrons* [interaktyvus]. 18 June 2022 [žiūrėta 2023-05-15]. Prieiga per: https://www.barrons.com/articles/bitcoin-price-crashing-51655567284
50. KOVACH, Steve. Tesla buys $1.5 billion in bitcoin, plans to accept it as payment. *CNBC* [interaktyvus]. 8 February 2021 [žiūrėta 2023-05-15]. Prieiga per: https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html
51. FRANKENFIELD, Jake. What Is a Block in the Crypto Blockchain, and How Does It Work? *Investopedia* [interaktyvus]. 11 June 2014 [žiūrėta 2023-05-15]. Prieiga

per: https://www.investopedia.com/terms/b/block-bitcoin-block.asp#:~:text=by%20Julius%20Mansa-,What%20Is%20a%20Block%20(Blockchain%20Block)?,validated,%20the%20block%20is%20closed.

52. HAYES, Adam. Blockchain Facts: What Is It, How It Works, and How It Can Be Used. *Investopedia* [interaktyvus]. 13 June 2014 [žiūrėta 2023-05-15]. Prieiga per: https://www.investopedia.com/terms/b/blockchain.asp
53. How bitcoin transactions work | How Do Bitcoin and Crypto Work? | Get Started with Bitcoin.com. *Buy Bitcoin & cryptocurrency | Wallet, news, education* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/#2/
54. Bitcoin price history chart since 2009 | 5yearcharts. *5yearcharts* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.5yearcharts.com/bitcoin-price-history-charts-and-milestones/
55. ANTE, Lennart. How Elon Musk's Twitter activity moves cryptocurrency markets. *Technological Forecasting and Social Change* [interaktyvus]. 2023, **186**, 122112 [žiūrėta 2023-05-15]. ISSN 0040-1625. Prieiga per: doi:10.1016/j.techfore.2022.122112
56. KOVACH, Steve. Tesla buys $1.5 billion in bitcoin, plans to accept it as payment. *CNBC* [interaktyvus]. 8 February 2021 [žiūrėta 2023-05-15]. Prieiga per: https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html
57. HAYES, Adam. CoinJoin: What it is, How it Works, Privacy Considerations. *Investopedia* [interaktyvus]. 30 October 2016 [žiūrėta 2023-05-15]. Prieiga per: https://www.investopedia.com/terms/c/coinjoin.asp
58. SUN, Xiaowen, Tan YANG, and Bo HU. LSTM-TC: Bitcoin coin mixing detection method with a high recall. *Applied Intelligence* [interaktyvus]. 2021 [žiūrėta 2023-05-15]. ISSN 1573-7497. Prieiga per: doi:10.1007/s10489-021-02453-9
59. DI FRANCESCO MAESA, Damiano, Andrea MARINO, and Laura RICCI. Data-driven analysis of Bitcoin properties: exploiting the users graph. *International Journal of Data Science and Analytics* [interaktyvus]. 2017, **6**(1), 63–80 [žiūrėta 2023-05-15]. ISSN 2364-4168. Prieiga per: doi:10.1007/s41060-017-0074-x
60. What is cluster analysis? *TIBCO Software* [interaktyvus], [žiūrėta 2023-05-15]. Prieiga per: https://www.tibco.com/reference-center/what-is-cluster-analysis
61. Clustering in Machine Learning - Javatpoint. *www.javatpoint.com* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.javatpoint.com/clustering-in-machine-learning
62. CONTRIBUTORS TO WIKIMEDIA PROJECTS. Cluster analysis - Wikipedia. *Wikipedia, the free encyclopedia* [interaktyvus]. 21 May 2004 [žiūrėta 2023-05-15]. Prieiga per: https://en.wikipedia.org/wiki/Cluster_analysis
63. WOODMAN, Ben. Cluster Analysis for Marketing Segmentation in Tableau: Who Wants Unfashionable Shoes? *Linkedin* [interaktyvus]. 2016 [žiūrėta 2023-05-15]. Prieiga per: https://www.linkedin.com/pulse/cluster-analysis-marketing-segmentation-tableau-who-wants-ben-woodman/
64. Orientuotieji grafai, Topologinis rikiavimas — Informatikos olimpiados: algoritmai ir taikymo pavyzdžiai. *Informatikos olimpiados: algoritmai ir taikymo pavyzdžiai —*

Informatikos olimpiados: algoritmai ir taikymo pavyzdžiai [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://inf-knyga.nmakademija.lt/lt/latest/09_orientuoti_grafai.html

65. Ekonometrika [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: http://www.ilab.lt/stabingiene/sk2_1.html
66. K-Means. *TowardsMachineLearning* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://towardsmachinelearning.org/k-means/
67. Elbow Method for optimal value of k in KMeans - GeeksforGeeks. *GeeksforGeeks* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.geeksforgeeks.org/elbow-method-for-optimal-value-of-k-in-kmeans/
68. How to interpret mean of Silhouette plot? *Cross Validated* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://stats.stackexchange.com/questions/10540/how-to-interpret-mean-of-silhouette-plot
69. klasterinė analizė. *Titulinis - Visuotinė lietuvių enciklopedija* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.vle.lt/straipsnis/klasterine-analize/
70. DBSCAN Algorithm Clustering in Python. *Engineering Education (EngEd) Program | Section* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.section.io/engineering-education/dbscan-clustering-in-python/
71. Bitcoin. *CoinDesk: Bitcoin, Ethereum, Crypto News and Price Data* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.coindesk.com/price/bitcoin/
72. What is a bull or bear market? *Coinbase* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.coinbase.com/learn/crypto-basics/what-is-a-bull-or-bear-market
73. Block timestamp - Bitcoin Wiki. *Bitcoin Wiki* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://en.bitcoin.it/wiki/Block_timestamp#:~:text="Network-adjusted%20time"%20is,within%20an%20hour%20or%20two.
74. OPTECH, Bitcoin. Child pays for parent (CPFP). *Bitcoin Optech* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://bitcoinops.org/en/topics/cpfp/
75. CoinMarketCap. Today's Cryptocurrency Prices by Market Cap. *CoinMarketCap* [interaktyvus]. N.d. [žiūrėta 2023-05-13]. Prieiga per: https://coinmarketcap.com/
76. Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap. *CoinMarketCap* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://coinmarketcap.com/
77. How Many Bitcoins Are There? - NerdWallet. *NerdWallet* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.nerdwallet.com/article/investing/how-many-bitcoins-are-there#:~:text=Bitcoin%20adds%20a%20new%20block,coins%20are%20minted%20each%20day.
78. How Many Blocks Are in a Blockchain? *Blockchain-Based Timestamping | OriginStamp* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://originstamp.com/blog/how-many-blocks-are-in-a-blockchain/#:~:text=Every%20valid%20block%20comprises%20a,turns%20into%20a%20verified%20transaction.
79. Ekonominės veiklos rūšių klasifikatorius | VĮ Registrų centras. *VĮ Registrų centras | VĮ Registrų centras* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.registrucentras.lt/jar/fa/klasif/v_rusys.php?kla_nr=1

80. CRAIG K, Elwell. Bitcoin: Questions, Answers, and Analysis of Legal Issues. *Congressional Research Service* [interaktyvus]. 2015 [žiūrėta 2023-05-15]. Priega per: https://www.everycrsreport.com/files/20150128_R43339_c87ebab0d56355eeb88495bf023adadb06511096.pdf
81. PERKINS W, David. Cryptocurrency: The Economics of Money and Selected Policy Issues. *Congressional Research Service* [interaktyvus]. 2020 [žiūrėta 2023-05-15]. Priega per: https://www.everycrsreport.com/files/20200409_R45427_8469ceaa641685c78bf188b7e5fdbb23004507a4.pdf
82. Bitcoin Transactions Per Day. *YCharts - Financial Research and Proposal Platform* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://ycharts.com/indicators/bitcoin_transactions_per_day
83. The Average Number of Credit Card Transactions Per Day & Year - CardRates.com. *CardRates.com* [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.cardrates.com/advice/number-of-credit-card-transactions-per-day-year/#:~:text=There%20were%20368.92%20billion%20purchase,every%20day%20around%20the%20world.
84. SEETHARAMAN, A., et al. Impact of Bitcoin as a World Currency. *Accounting and* Finance Research [interaktyvus]. 2017, 6 (2), 230 [žiūrėta 2023-05-15]. ISSN 1927-5994. Prieiga per: doi:10.5430/afr.v6n2p230
85. Cryptocurrency in Construction: How Contractors Are Using Digital Currency to Get Paid. Levelset [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.levelset.com/blog/cryptocurrency-in-construction/
86. TEAM, The BitPay. What Can You Buy with Bitcoin? How to Spend Bitcoin. BitPay Blog [interaktyvus]. 2023 [žiūrėta 2023-05-15]. Prieiga per: https://bitpay.com/blog/what-can-you-buy-with-bitcoin/#:~:text=You%20can%20buy%20domain%20names,your%20web%20services%20with%20crypto.
87. Palazzo Versace Dubai. Palazzo Versace Dubai [interaktyvus]. 2022 [žiūrėta 2023-05-15]. Prieiga per: https://www.palazzoversace.ae/press/palazzo-versace-dubai-now-accepts-cryptocurrency-payments
88. HAMACHER, Adriana. Norwegian Air to accept bitcoin, opening crypto exchange. Yahoo Finance [interaktyvus]. 2019 [žiūrėta 2023-05-15]. Prieiga per: https://finance.yahoo.com/news/norwegian-air-accept-bitcoin-opening-104716311.html#:~:text=One%20of%20Europe's%20leading%20budget,(DN)%20newspaper%20reported%20yesterday.
89. Airlines that accept Bitcoin and Altcoins. Top Bitcoin and other Crypto Payment Processor [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://coingate.com/blog/post/travel-sites-accept-bitcoin-altcoins
90. WANG, Merrick. Bitcoin and its impact on the economy. arXiv [interaktyvus]. 2020 [žiūrėta 2023-05-15]. Prieiga per: https://arxiv.org/abs/2010.01337

91. Pay for College with Crypto -. Upromise | Earn cash back towards your 529 college savings plan [interaktyvus]. [žiūrėta 2023-05-15]. Prieiga per: https://www.upromise.com/articles/pay-for-college-with-crypto/
92. BBC NEWS. Microsoft to accept payments made in bitcoins. *BBC News* [interaktyvus]. 11 December 2014 [žiūrėta 2023-05-15]. Prieiga per: https://www.bbc.com/news/technology-30377654
93. ANTE, Lennart. The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum. *FinTech* [interaktyvus]. 2022, **1**(3), 216–224 [žiūrėta 2023-05-15]. ISSN 2674-1032. Prieiga per: doi:10.3390/fintech1030017