Kauno technologijos universitetas

Informatikos fakultetas

Kriptovaliutų transakcijų analizės metodas

Baigiamasis magistro projektas

Linas Pocius

Projekto autorius

Prof. Dr. Šarūnas Grigaliūnas

Vadovas

Kaunas, 2025

Kauno technologijos universitetas

Informatikos fakultetas

Kriptovaliutų transakcijų analizės metodas

Baigiamasis magistro projektas

Informacijos ir informacinių technologijų sauga (6211BX008)

Linas Pocius

Projekto autorius

Prof. Dr. Šarūnas Grigaliūnas

Vadovas

Doc. Nerijus Morkevičius

Recenzentas

Kaunas, 2025

Kauno technologijos universitetas

Informatikos fakultetas

Linas Pocius

Kriptovaliutų transakcijų analizės metodas

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 mokėjęs (-usi);

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

Linas Pocius

Patvirtinta elektroniniu būdu

Pocius Linas. Kriptovaliutų transakcijų analizės metodas. Magistro studijų baigiamasis projektas; vadovas doc. dr. Šarūnas Grigaliūnas; Kauno technologijos universitetas, informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informacijos ir informacinių technologijų sauga.

Reikšminiai žodžiai: Bitcoin, pinigų plovimo prevencija, kibernetiniai nusikaltimai, mašininis mokymasis.

Kaunas, 2025. 70 p.

Santrauka

Kriptovaliutos tampa svarbia ekonomikos dalimi. Net ketvirtis *Bitcoin* piniginių dalyvauja nelegaliose veiklose, beveik kas antras pervedimas tinkle atliekamas piktavalių. Rinkoje auga kriptovaliutų piniginių srautų reguliavimo poreikis, tyrėjams trūksta įrankių galinčių atlikti išsamią piniginių analizę.

Šiame darbe tiriamos mašininio mokymosi galimybės analizuoti *bitcoin* tinklo finansines operacijas. Pagrindiniai darbo uždaviniai yra: atlikti susijusios literatūros apžvalgą, paruošti duomenų rinkinį, ištreniruoti modelius, išskirti geriausią, panaudoti jį įrankio, gebančio klasifikuoti *bitcoin* finansines operacijas, sukūrimui.

Sukurtas duomenų rinkinys tinkamas treniruoti modelius, kurie gebėtų atlikti finansinių operacijų analizę tikru laiku naudojant realius, modeliui nematytus *bitcoin* tinklo duomenis. Panaudoti trys klasifikavimo algoritmai (atsitiktinis miškas, *ADA Boost*, *XG Boost*). Realių finansinių operacijų klasifikavimo metu atliekama stebinio *SHAP* analizė, gebanti paaiškinti kurie finansinės operacijos požymiai lėmė modelio sprendimą. Geriausi rezultatai gauti naudojant *XG Boost* algoritmą, svarbiausias požymis – finansinės operacijos mokestis. Naudojantis šiuo modeliu sukurtas intuityvus įrankis finansinių nusikaltimų *bitcoin* tinkle tyrėjams.

Pocius Linas. Method for Cryptocurrencies Transaction Analysis. Master's Final Degree Project; supervisor Assoc. Prof. Dr. Šarūnas Grigaliūnas; Faculty of Informatics, Kaunas University of Technology.

Study field and area (study field group): Information and Information Technology Security.

Keywords: Bitcoin, Anti-Money laundering, cybercrime, machine learning.

Kaunas, 2025. 70 pages.

Summary

Cryptocurrencies are becoming an important part of the economy. As much as a quarter of Bitcoin wallets are involved in illegal activities, almost every second transfer on the network is made by malicious actors. The market is growing in need of regulation of cryptocurrency cash flows, and investigators lack tools capable of performing a detailed analysis of crypto wallets.

This paper investigates the possibilities of machine learning for analyzing bitcoin network transactions. The main objectives of this paper are to conduct a review of relevant literature, prepare a dataset, train models to select the best one, and use it to create a tool capable of detecting illegal *bitcoin* transactions.

The created dataset is suitable for training models that would be able to perform transaction analysis in real time using real, unseen bitcoin network data. Three classification algorithms were used (random forest, ADA Boost, XG Boost). During the classification of real transactions, *SHAP* analysis of the observation is performed, which can explain which transaction features determined the model's decision. The best results were obtained using the *XG Boost* algorithm, the most important feature being the transaction fee. Using this model, an intuitive tool with a user interface has been created for investigators of financial crimes on the *bitcoin* network.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

BTC – kripto valiuta *bitcoin*

CoC – pasitikėjimo grandinė (angl. *Chain of Custody*)

DI – dirbtinis intelektas

FP – klaidingai teigiami (angl. *False positives*)

IoT – daiktų internetas (angl. *Internet of things*);

Json – duomenų saugojimo formatas (angl. *JavaScript Object Notation*)

LTEC – Lietuvos teismo ekspertizės centras

MiCA – Europos sąjungoje taikomas kriptoturto rinkų reglamentas (angl. *Markets in Crypto-Assets Regulation*)

ROC kreivė – jautrumo ir specifiškumo charakteristikos kreivė (angl. *Receiver operating characteristic*)

TN – teisingai neigiami (angl. *True negative*s)s

XAI – paaiškinamas dirbtinis intelektas (angl. *explainable artificial intelligence*)

Terminai:

ADA Boost – atsitiktinio miško stiprinimo (angl. *Boosting*) tipo mašininio mokymosi algoritmas, kurio pavadinimo akronimas reiškia adaptyvus stiprinimas (angl. *Adaptive boosting*)

Blokų grandinės technologija – paskirstytos duomenų bazės tipas, o tai reiškia, kad atnaujinti blokų grandinę gali bet kuris tinklo dalyvis (mazgas)

SHAP analizė – dirbtinio intelekto modelių sprendimų interpretavimo metodas.

XG Boost – atsitiktinio miško stiprinimo (angl. *Boosting*) tipo mašininio mokymosi algoritmas, kuris implementuoja gradientinį stiprinimą.

Įvadas

Aktualumas. Šiais laikais vis labiau augant skaitmeninių prietaisų naudojimui, auga ir jų įtraukimas į nelegalias veiklas. Tokiems nusikaltimams, vadinamiems elektroniniais nusikaltimais (angl. *cybercrimes*) tirti buvo sukurta nauja ekspertinių tyrimų šaka – skaitmeninė kriminalistika. Viena opiausių elektroninių finansų spragų, kuria naudojasi elektroniniai nusikaltėliai – blokų grandinėmis pagrįstų kriptovaliutų naudojimas įvairiems nusikaltimams atlikti arba juos finansuoti. Dėl savo anonimiškumo ir decentralizuoto pobūdžio kriptovaliutos neretai naudojamos pinigams plauti, terorizmui finansuoti, narkotikų, ginklų prekybai. Kriptovaliutų ekosistemai augant didėja teisėsaugos institucijų tyrėjų poreikis įrankiams ir naujoms metodikoms, kurios gebėtų sparčiai bei patikimai analizuoti kriptovaliutų pervedimus, taip palengvindamos kovą su nusikalstamumu.

Problema. Kriptovaliutų tinklai nėra pakankamai reguliuojami, tyrėjams trūksta patogių įrankių tinklams analizuoti.

Projekto tikslas. Panaudojant mašininio mokymosi algoritmus sukurti įrankį aptinkantį nelegalias kriptovaliutų finansines operacijas.

Uždaviniai:

- Atlikti mokslinės literatūros, nagrinėjančios skaitmeninę kriptovaliutų kriminalistiką ir analizę apžvalgą
- Surasti ir paruošti duomenų rinkinį modelių treniravimui
- Ištreniruoti modelius, realizuoti prototipą
- Analizuoti, interpretuoti bei vizualizuoti gautus rezultatus

1. Literatūros analizė

1.1. Kriptoturto skaitmeninė kriminalistika

Skaitmeninė kriminalistika – tai informacijos išgavimas iš skaitmeninių įrenginių ir sistemų bei išgautos informacijos analizavimo praktika. Ši praktika dažnai naudojama tiriant elektroninius nusikaltimus ar incidentus, kurių metu naudojamasi kompiuteriais, išmaniaisiais telefonais ir kitais skaitmeniniais įrenginiais. Tokiu būdu stengiamasi nustatyti įvykių seką, nustatyti susijusius asmenis ir nustatyti bylos faktus.

Skirtingai nei tradicinė skaitmeninė kriminalistika, kriptoturto skaitmeninė kriminalistika reikalauja specifinių metodų ir įrankių, skirtų analizuoti blokų grandinių operacijas, kriptovaliutų pinigines ir kitus skaitmeninius kriptoturto artefaktus. Ši praktika yra būtina tiriant nusikaltimus, susijusius su neteisėtai atliktais veiksmais kriptovaliutų tinkluose. Tokiu būdu siekiama atsekti lėšų srautus, nustatyti susijusias šalis bei surinkti įrodymus teisiniam procesui.

1.2. Kriptoturto skaitmeninės kriminalistikos darbo eiga

Kriptoturto skaitmeninė kriminalistika apima specifinius žingsnius pritaikytus blokų grandinių technologijų galimybėms (1 pav.):

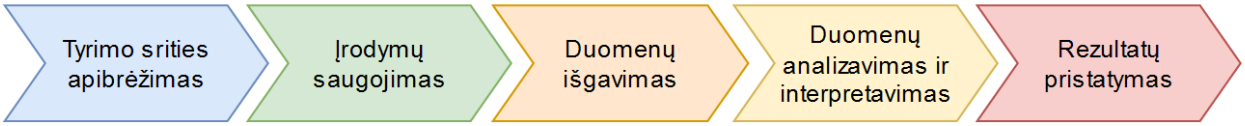
1. Tyrimo apimties apsibrėžimas – nustatomi blokų grandinių tinklai, kriptovaliutų piniginės, finansinės operacijos ar išmanieji kontraktai kurie yra tyrimo objektas.

2. Įrodymų saugojimas – informacija naudojama tyrime turi būti saugoma taip, kad būtų išsaugotas įrodymų vientisumas ir autentiškumas. Atsižvelgiant į blokų grandinės decentralizuotą pobūdį įrodymų saugojimas apima ne tik fizinių (pvz. serverių ar kompiuterių) objektų saugojimą, bet ir grandinės duomenų kopijų darymą, metaduomenų įrašymą.

3. Duomenų išgavimas – analitikai, naudoja specializuotus įrankius ir metodus, tam kad ištirtų įrenginių / sistemų duomenis ir gautų panaudojamą informaciją. Tai gali apimti failų sistemų analizę, ištrintų duomenų atkūrimą, blokų grandinių duomenų srauto susisteminimą. Kriptoanalizės metu duomenys išgaunami naudojant įvairias programavimo sąsajas, jei finansinės operacijos vyko per kriptoturto keityklas teisėsaugos institucijos gali reikalauti keityklas pateikti duomenis reikalingus tyrimui.

4. Duomenų analizavimas ir interpretavimas – po duomenų išgavimo, skaitmeninės kriminalistikos analitikai juos turi interpretuoti, tai gali apimti modelių kūrimą, koreliacijų ar kitų rodiklių, kurie gali padėti nustatyti bylos faktus nustatymą. Kriptoanalizės metu grandinėse ieškoma anomalijų, analizuojami ryšiai tarp keityklų, piniginių adresų.

5. Rezultatų pristatymas – skaitmeninės kriminalistikos analitikai gali būti kviečiami pateikti savo išvadas ataskaitoje, teisme arba kitoms tyrime dalyvaujančioms šalims. Jie turi sugebėti aiškiai ir tiksliai perteikti savo išvadas ir paaiškinti tyrimo metu naudojamus įrankius ir metodus.



1 pav. Skaitmeninės kriminalistikos tyrimo proceso fazės

Panaši skaitmeninės kriminalistikos metodologija pateikiama 2019 metų F. Amato ir jos kolegų straipsnyje[5]. Jame aptariama kaip teismo ekspertizės tyrimo gavybos, išsaugojimo, analizės ir dokumentavimo procesas gali būti pagerintas naudojant sukurtą karkasą, kuris padėtų tyrėjams atlikti jų darbą, susiejant įrodymus, surinktus naudojant įvairias teismo ekspertizės priemones.

1.3. Kriptoturto duomenų autentiškumo nustatymo metodai

Pirminė skaitmeninės analizės problema – informacijos autentiškumo nustatymas. 2022 metų moksliniame straipsnyje buvo aprašytos autentiškumo nustatymo problemos ir galimi sprendimo būdai informacijos autentiškumui nustatyti[3]. Straipsnyje pabrėžiama, kad elektroninių įrodymų kilmė dažnai vertinama su dideliu įtarumu. Pagrindinė siunčiama žinutė, kad kiekvienas naujai kuriamas skaitmeninės analizės metodas turi būti kruopščiai patikrintas per legalumo prizmę, atsakant į klausimą ar metodą bus galima panaudoti teisme? Šis teisinis metodų kūrimo aspektas yra aktualus iki šiol.

Kriptoturto duomenų autentiškumo nustatyme, blokų grandinės duomenų analizė kelia unikalius iššūkius, kadangi duomenys yra decentralizuoti, o jų vientisumas yra esminis reikalavimas teisiniam procesui. Pasitikėjimo grandinė yra vienas iš pagrindinių metodų, kuriuo siekiama užtikrinti skaitmeninių įrodymų, susijusių su kriptoturtu vientisumą. Kriptoturto skaitmeninės kriminalistikos kontekste pasitikėjimo grandinė gali būti naudojama saugiam ir nekintamam skaitmeninių įrodymų įrašui sukurti. Tai galėtų apimti skaitmeninių įrodymų saugojimą grandinėje kartu su metaduomenimis, tokiais kaip įrodymų surinkimo data ir laikas, vieta, iš kurios jie buvo surinkti. Pasitikėjimo grandinė yra ne kas kita, kaip nuosekli dokumentacija, kurios įrašuose renkama informacija nuo duomenų surinkimo iki jų pateikimo kaip įrodymo teisminiame procese ar kituose tarnybiniuose veiksmuose. Pasitikėjimo grandinė yra svarbi, ne tik dėl to, kad padeda užtikrinti įrodymų vientisumą ir autentiškumą, bet ir dėl aiškių nurodymų, kas tvarkė įrodymus ir kas su jais buvo padaryta.

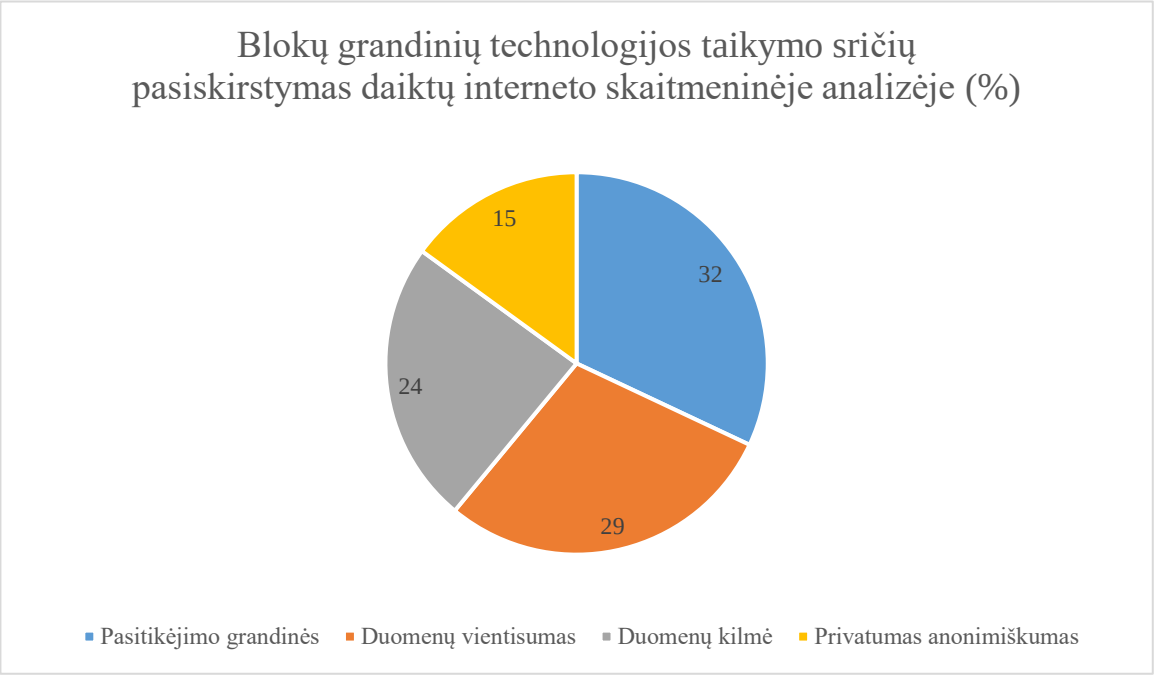
Vienas naujesnių blokų grandinės principu paremtų pasitikėjimo grandinės projektų *LEChain*[17]. Šis projektas liudytojų tapatybei patvirtinti naudoja trumpus atsitiktinius parašus, pasitelkia tikslią prieigos kontrolę, pagrįstą šifravimu (*CP-ABE*), kad įkeltų, pasiektų ir atnaujintų įrodymus, taip pat kuria saugų balsavimo metodą, kad apsaugotų prisiekusiųjų privatumą. Sprendimas koncentruojasi į privatumo išsaugojimą, tiek prisiekusiųjų, tiek liudininkų davusių parodymus. Siekdami įrodyti sukurto prototipo efektyvumą, autoriai paleidžia prototipą Ethereum1test tinkle.

Svarbu pažymėti, kad nors blokų grandinių technologija gali sustiprinti skaitmeninių įrodymų saugojimo grandinės vientisumą, tai nėra 100% patikimas sprendimas ir turi būti naudojamas kartu su kitais metodais ir technikomis siekiant užtikrinti įrodymų patikimumą.

1.4. Blokų grandinėmis grįsti daiktų interneto skaitmeninės analizės metodai

Blokų grandinių technologija gali būti taikoma ne tik pasitikėjimo grandinės projektams. Pagal 2022 metų mokslinę literatūrą nagrinėjantį straipsnį, daiktų interneto (angl. *IoT*) srityje blokų grandinių taikymo pasiskirstymas gali būti apibrėžtas tokiais rodmenimis (2 pav.)[4]:

- 32% - pasitikėjimo grandinių (angl. *Chain of custody*) sprendimai.
- 29% - duomenų vientisumą (angl. *integrity*) užtikrinantys sprendimai.
- 24% - duomenų kilmę (angl. *data provenance*) užtikrinantys sprendimai.
- 15% - privatumą ir anonimiškumą (angl. *privacy and identity anonimity*) užtikrinantys sprendimai.



2 pav. Blokų grandinių sprendimų pasiskirstymas daiktų interneto srityje

Visgi, atsirandant vis daugiau skaitmeninę analizę tobulinančių metodų, iškyla poreikis ir anti-kriminalistikos metodams. Atlikti nusikaltimai daiktų interneto srityje dažniausiai bandomi užglaistyti šiomis technikomis[13]:

- Duomenų slėpimas (šifravimas ar steganografija) – technika naudojama paslėpti bet kokius įrodymus ar pėdsakus. Tai labai apsunkina kriminalistinius tyrimus.
- Saugus ištrynimas – technika visam laikui ištrinanti duomenis, perrašant juos atsitiktiniais duomenimis. Taip užtikrinama, kad duomenys nebus atkurti. Visgi dauguma įrankių negali pilnai ištrinti duomenų, dalį jų vis tiek įmanoma atkurti.
- Laiko žymos keitimas (angl. *timestomping*) – laiko žymos keitimas, kad atrodytų, jog įrašai ar įrodymai buvo sukurti kitu laiku.
- Fizinis duomenų sunaikinimas – fizinis duomenų saugyklos (disko, atmintinės) sunaikinimas sudeginant ar kitais būdais sugadinant / sunaikinant.

Tobulėjant anti-kriminalistikos metodams, atsiranda poreikis ir anti-anti-kriminalistikai. Tai tokie metodai ar technikos kurios geba analizuoti duomenis ir aptikti klastojimo ir kitus neteisėtus pėdsakus. Jean-Paul A. Yaacoub ir jo kolegų 2022 metais parašytas straipsnis, aprašantis pažengusias skaitmeninės kriminalistikos technikas, tolimesniems tyrimams rekomenduoja eksperimentuoti su mašininio mokymosi sprendimais, norint aptikti anti-kriminalistikos technikas[13].

1.5. Mašininis mokymasis skaitmeninėje analizėje

Augant daiktų internetui, debesų technologijoms ir ūko kompiuterijai, tinklai tampa eksponentiškai sudėtingesni. Šią problemą dar labiau apsunkina saugojimo įrenginių talpa ir prie tinklų prijungtų, autonomiškai veikiančių įrenginių įvairovė. Šių problemų sprendimams rasti, 2024 metų Jungtinės Karalystės Londono Metropoliteno universiteto mokslininkai rekomenduoja tyrinėti dirbtinio intelekto pritaikymą skaitmeninėje kriminalistikoje[7].

Mašininis mokymasis yra dirbtinio intelekto (DI) poaibis, apimantis algoritmų ir statistinių modelių naudojimą. Mašininis mokymasis leidžia kompiuteriams mokytis ir taip pagerinti savo efektyvumą. Skaitmeninėje kriminalistikoje mašininis mokymasis gali būti naudojamas tam tikrų užduočių automatizavimui. Kai kurie galimi mašininio mokymosi pritaikymo būdai:

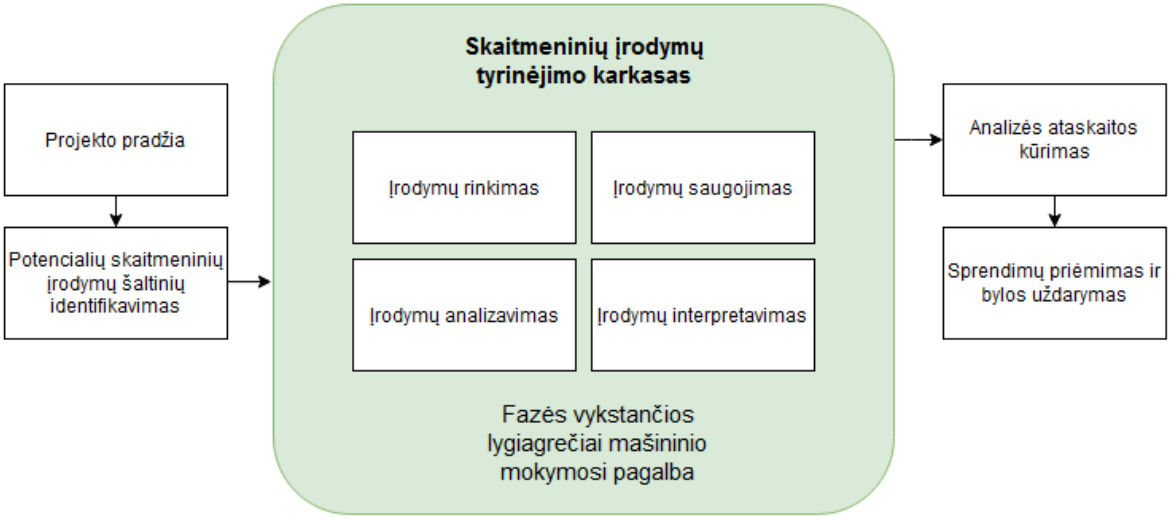
- Automatizuota duomenų analizė: Mašininio mokymosi algoritmai gali būti naudojami norint greitai ir tiksliai analizuoti didelius duomenų kiekius, todėl teismo ekspertai gali efektyviau nustatyti svarbius įrodymus. Vienas pavyzdžių – konfiskuotas kompiuteris, visų jo failų nagrinėjimas užtruktų itin daug laiko, nes dauguma duomenų nėra tiesiogiai susiję su tyrimu, čia padėti gali automatizuoti įrankiai, surandantys tyrimui aktualius artefaktus[11].

- Skaitmeninių įrodymų klasifikavimas: Mašininio mokymosi algoritmai gali būti išmokyti klasifikuoti skaitmeninius įrodymus pagal tam tikras savybes ar ypatybes, pvz., failo tipą arba turinį. Mašininio mokymosi algoritmų palyginimą nustatant kaltinančius įrodymus, atsekant istorinę failų sistemos veiklą nagrinėjamas Imam Abdulrahman Bin Faisal universiteto mokslininkai savo 2019 metais publikuotame straipsnyje[23].

- Anomalijų aptikimas: mašininio mokymosi algoritmai gali būti naudojami norint nustatyti neįprastus ar įtartinus duomenų modelius, kurie gali rodyti atitinkamų įrodymų buvimą.

- Spėjamoji analizė: mašininio mokymosi algoritmai gali būti naudojami tam tikrų įvykių ar rezultatų tikimybei numatyti remiantis ankstesniais duomenimis.

Mašininio mokymosi pritaikymą daiktų interneto srityje nagrinėjantis Victor R. Kebande ir jo kolegos 2020 metais priėjo išvadų, kad tiesioginių duomenų apdorojimo srityje prižiūrimo mokymosi algoritmai taps vis svarbesni[15]. Visgi, daiktų internetas nėra vienintelė didžiųjų duomenų sritis, kurioje kuriami dirbtinio intelekto sprendimai. Giliojo mokymosi sprendimai gali būti pritaikomi daugumoje skaitmeninių tyrimų fazių (3 pav.).



3 pav. Tyrėjų sukurtas skaitmeninių įrodymų tyrimų karkasas

Tyrėjų pasiūlytas giliojo mokymosi kognityvinius skaičiavimus atliekantis karkasas galėtų būti pritaikomas visose skaitmeninės kriminalistikos tyrimo fazėse (1 pav.)[14].

1.6. Problemos kylančios naudojant mašininį mokymąsi skaitmeninėje kriminalistikoje

Visgi mašininio mokymosi algoritmai turi trūkumų - nusikaltimų tyrėjai susirūpinę dėl dirbtinio intelekto modelių skaidrumo ir jų tinkamumo naudoti:

- Paaiškinamumo trūkumas: kai kurie mašininio mokymosi algoritmai nėra lengvai interpretuojami, todėl sunku suprasti, kodėl ir kaip jie priėmė konkretų sprendimą ar prognozę. Nors dirbtinio intelekto modeliai yra aprašyti matematiškai ir statistiškai, tai gali būti problema atliekant teismo ekspertizę, kai svarbu suprasti išvados motyvus.

- Teisinis priimtinumas: kai kuriais atvejais mašininio mokymosi analizės rezultatai gali būti nepriimtini kaip įrodymai teisminiame procese dėl rezultatų patikimumo ir tikslumo. Šis faktorius priklauso nuo šalies kurioje vyksta teismo procesas įstatymų.

Šias problemas sprendžia paaiškinamas dirbtinis intelektas (angl. *Explainable Artificial Intelligence (XAI)*).

1.7. Paaiškinamas dirbtinis intelektas

Paaiškinamasis dirbtinis intelektas (dar kitaip vadinamas interpretuojamuoju DI) yra dirbtinio intelekto tipas, kurio pagrindinė savybė yra gebėjimas paaiškinti savo sprendimus, prognozes ar veiksmus. Paaiškinamojo svarbą skaitmeninėje kriminalistikoje pabrėžia ir 2022 metais publikuotas straipsnis apie DI naudojimą skaitmeninėje kriminalistikoje[10]. Paaiškinamasis dirbtinis intelektas siekia, kad dirbtinio intelekto sistemos būtų skaidresnės ir suprantamesnės, kad žmonės galėtų suprasti jų elgesį ir sprendimų priėmimo procesus ir jomis pasitikėtų. Keletas argumentų kodėl paaiškinamasis dirbtinis intelektas yra svarbi tyrinėjimo sritis skaitmeninėje kriminalistikoje:

- Pasitikėjimas: pateikdamos paaiškinimus dėl savo sprendimų, paaiškinamos dirbtinio intelekto sistemos gali įgauti pasitikėjimą.

- Skaidrumas: paaiškinamos dirbtinio intelekto sistemos gali papildyti dirbtinio intelekto sistemas padarydamos jas skaidresnes, o tai gali padėti užtikrinti, kad jos būtų naudojamos etiškai.

- Paaiškinamumas: XAI gali padėti lengviau suprasti dirbtinių intelekto sistemų sprendimų ir veiksmų motyvus, o tai gali būti naudinga gerinant našumą ir užtikrinant, kad būtų laikomasi nustatytų taisyklių.

Visgi pasiekti, kad dirbtinio intelekto sistemos būtų paaiškinamos gali būti sunku, nes dauguma kriminalistiniuose tyrimuose naudojamų sprendimų nėra atvirojo kodo, ir padaryti jas programiškai skaidriomis beveik neįmanoma neatskleidžiant įmonės paslapčių. Nerimą kelia tai, kad bandymai pernelyg supaprastinti dirbtinio intelekto sprendimus didinant jų paaiškinamumą gali apriboti mokslinį tobulėjimą[29].

Pagrindiniai save aiškinančio dirbtinio intelekto tipai:

- Save paaiškinantys modeliai (angl. *Inherently interpretable models*)

    - Sprendimų medžiai – medžio struktūra aiški ir nesunkiai interpretuojama, kiekvienas mazgas atspindi sprendimą pagal tam tikrą požymį, medžio lapai atspindi klasifikavimo prognozę. Visgi kuomet sprendimų medžiai naudojami dideliais kiekiais, kaip atsitiktinio miško atveju, kiekvieną medį atskirai nagrinėti tampa sunku.

    - Regresijos modeliai – kiekvienam požymiui priskiriami koeficientai, kurie nurodo kuria kaip didėjant požymio vertei didėja prognozuojamos klasės vertė. Yra keli pagrindiniai regresijos modelių tipai: linijinė regresija, naudojama kuomet prognozuojamas kintamasis yra tolydus, gali įgyti reikšmes konkrečiame intervale ir logistinė, naudojama kuomet prognozuojamas kintamasis yra dvireikšmis.

- Po fakto aiškinami modeliai (angl. *Post-hoc explanations*) – naudojami siekiant paaiškinti sudėtingus juodosios dėžės tipo modelius, kurie nėra savaime interpretuojami[27].

    - *LIME* (angl. *Local interpretable model-agnostic explanations*) analizė – veikia minimizavimo principu, keičia duomenis kurie buvo panaudoti apmokyti modelį iškraipydamas juos ir žiūri ar modelio prognozė pasikeitė. Taip LIME gali suprasti kurie požymiai buvo svarbiausi atliktam sprendimui[33].

    - *SHAP* analizė – naudoja žaidimų teorijos pagrindu grįsta analizė, kuri siekia įvertinti kiekvieno požymio indelį priimant sprendimus[25].

    - Dalinių priklausomybių grafikai – vizualizuoja vieno ar kelių nagrinėjamų požymių reikšmes ir parodo kaip vidutiniškai keičiasi prognozuojamas rezultatas, priklausomai nuo nagrinėjamų požymių reikšmių.

    - Įvairios kitokio tipo vizualizacijos, pavyzdžiui šilumos žemėlapiai, naudojami apdorojant vaizdus – jie parodo kurie įvesties pikseliai, ar pikselių regionai turėjo įtakos priimant sprendimą.

Įvertinus paaiškinamojo DI tipus galima suprasti paaiškinimų svarbą, bei faktą, kad tai yra kertinė dirbtinio intelekto evoliucijos dalis, kuri tampa vis labiau reikalinga didžiųjų duomenų kontekste.

1.8. Metodai modeliai ir įrankiai

Analizuojant literatūrą, nagrinėjančią skaitmeninėje ekspertizėje naudojamus metodus, informacija buvo susisteminta į lentelę (1 lentelė.).

1 lentelė. Metodai, modeliai ir įrankiai naudojami skaitmeninėje ekspertizėje

Pavadinimas	**Sprendimas**	**Kas nepadengta (siūlymai tolesniam darbui)**
A comparison of machine learning techniques for file system forensics analysis[23]	**Modelis**. Tyrimu siekiama ištirti sukurtų mašininio mokymosi modelių pritaikomumą aptinkant skaitmeninius įrodymus.	Gauti rezultatai tebuvo patenkinami, raginama ieškoti geresnių mašininio mokymosi algoritmų.
Analyse digital forensic evidences through a semantic-based methodology and NLP techniques[5]	**Metodas.** Tyrime pristatoma metodologija, naudojanti teksto apdorojimo būdus. Metodologijos tikslas – palengvinti informacijos išgavimo ir paieškos iššūkius teismo ekspertizėje.	Mašininio mokymosi naudojimas multimedijos failų analizėje.
Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics[31]	**Metodas**. *Elliptic* patalpinto duomenų rinkinio analizė, siūlomi duomenų vizualizacijos metodai.	Rekomenduojama tyrinėti būdus, kaip padaryti finansines sistemas saugesnes.
Diverging deep learning cognitive computing techniques into cyber forensics[14]	**Įrankis**. *DLCF framework - Deep learning cyber-forensics framework*. Jo tikslas parodyti giliojo mokymosi (angl. *deep learning*) galimybes ir apribojimus skaitmeninėje ekspertizėje.	*Deep learning cognitive computing* technikos - kaip jos gali būti panaudotos ekspertizės analitikų tyrimų procesui valdyti.
LEChain: A blockchain-based lawful evidence management scheme for digital forensics[17]	**Metodas**. Blokų grandinėmis pagrįsta pasitikėjimo grandinės schema.	Siūloma plėtoti sukurtą įrankį ir daryti jį saugesnį.
Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity[21]	**Modelis**. Tyrimo metu analizuotas *Elliptic* duomenų rinkinys ir mašininio mokymosi metodų efektyvumas aptinkant nelegalias operacijas.	Siūloma pinigų plovimo prevencijos metodus naudojamus kriptovaliutų tinkluose pritaikyti ir kitose finansinėse sistemose, gerinti aptikimą *Bitcoin* tinkle.
Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments[15]	**Metodas**. Siūlomas naujas būdas daiktų interneto tyrimams. Sukurtas karkaso prototipas.	Toliau nagrinėti mašininio mašininio mokymosi metodų pritaikymo būdus tiesioginiam duomenų srautui.
Illegal activity detection on bitcoin transaction using deep learning[24]	**Modelis**. Dirbtinio intelekto modelis *Bitcoin* finansinių operacijų klasifikavimui ar jos legalios, ar ne.	Plėsti sukurtą algoritmą, pabandyti panašią analizę atlikti *Ethereum* tinkle.
Targeted Addresses Identification for Bitcoin with Network Representation Learning[18]	**Metodas**. Naudojamas mašininis mokymasis, kad ištraukti reikiamus atributus ir ištreniruoti nesubalansuotą multi-klasifikatorių.	Sukurti modeliai yra nuoseklūs, tai reiškia vienu laiko momentu sukurtas ML modelis, gali būti taikomas ir ateityje. Toliau įrodinėti šią prielaidą.
Dissecting Ethereum Blockchain Analytics: What We Learn from Topology and Geometry of the Ethereum Graph?[16]	**Metodas**. Pasiūlyti nauji konceptai - *Betti* limitai ir *Betti* ašis.	Tolimesni pasiūlyto koncepto tyrimai blokų grandinių taikyme.

Matoma, kad mašininis mokymasis yra svarbus skaitmeninės kriminalistikos įrankis, reikalaujantis tolimesnių tyrimų.

1.9. Blokų grandinių finansinės operacijos

Blokų grandinių sistemose, transakcijomis yra vadinamos naudotojo finansinės operacijos sistemoje. Kai naujas lėšų pervedimas yra inicijuojamas naudotojo, jis bus ištransliuotas į visus tinklo mazgus ir įtrauktas į naują bloką.

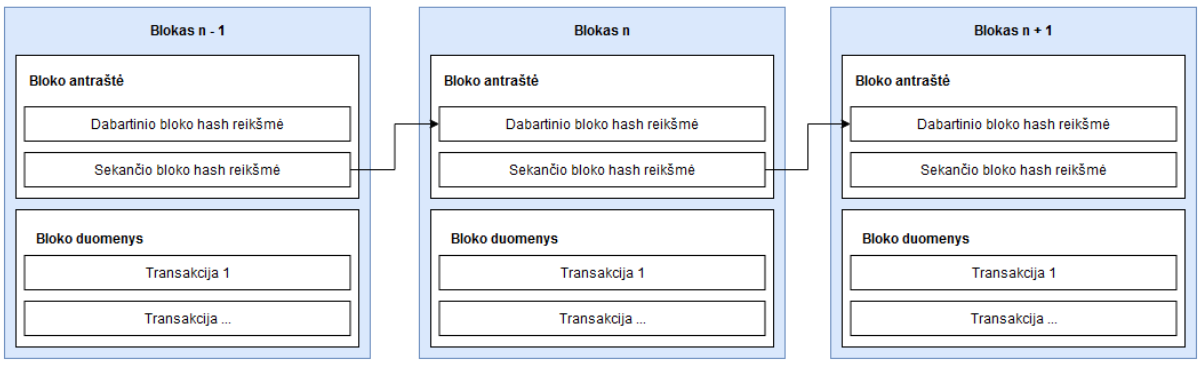
Kriptovaliutų ekosistemoje finansinė operacija įprastai susideda iš duomenų apie sandorį atliekančias šalis, bei su sandoriu susijusius duomenis ir metaduomenis:

- Siuntėjo ir gavėjo adresai – sandorio dalyvių adresai
- Operacijos suma – norima perduoti suma, tarkime *Bitcoin* tinkle mažiausias nedalomas skaitmeninio turto vienetas – *satoshi*, tai atitinka 0.00000001 BTC, reiškia mažiausia galima perduoti suma *Bitcoin* tinkle yra 1 *satoshi*‘s.
- Sandorio mokestis – nedidelis mokestis, kuris paprastai mokamas operacijų tikrintojams (angl. *miners*), kurie patikrina ir įrašo operaciją blokų grandinėje. Įprastai šis mokestis yra mokamas tokia pat kriptovaliuta kaip ir prieš tai minėta operacijos suma.
- Skaitmeninis parašas – kriptografinis parašas, naudojamas finansinės operacijos autentiškumui patikrinti. Jis padeda užtikrinti, kad operaciją atlieka skaitmeninio turto savininkas
- Laiko žymė – data ir laikas, kuomet operacija buvo įrašyta į blokų grandinę

Šios finansinės operacijos blokų grandinių technologijų pagalba jungiamos į blokus ir taip saugomos decentralizuotoje duomenų saugykloje.

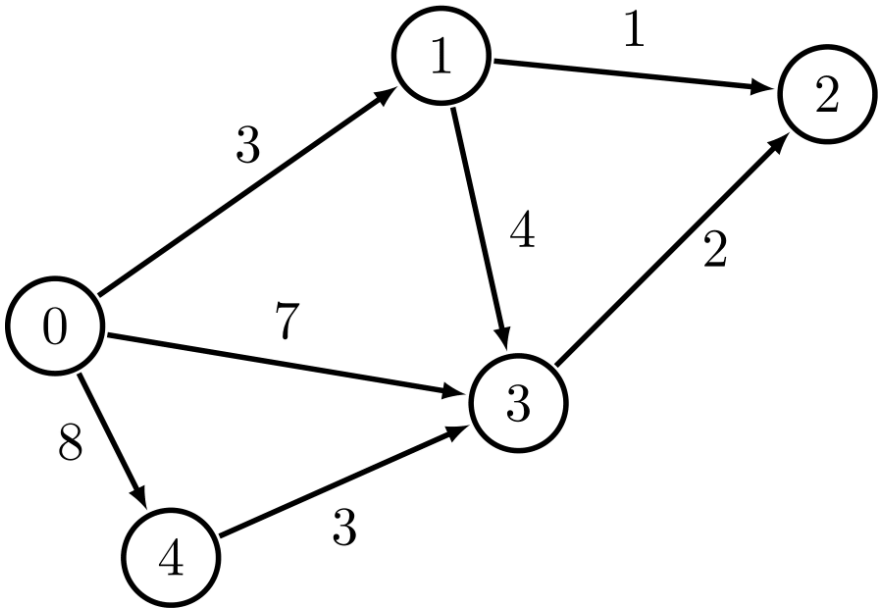
1.10. Finansinių operacijų struktūra blokų grandinėse

Blokų grandinės yra paskirstyta duomenų bazė, kurioje saugomi finansinių operacijų įrašai. Finansinės operacijos įrašomos į blokus, kurie sujungti grandine. Kiekvienas blokas turi finansinių operacijų įrašus ir maišos (angl. *hash*) funkcijos reikšmę, kuri atlieka identifikatoriaus paskirtį ir susieja bloką su ankstesniu. Taip sukuriamas visų blokų grandinėje įvykusių finansinių operacijų sąrašas (4 pav.)[2].



4 pav. Blokų grandinių struktūra

Kiekvieną *bitcoin* grandinės bloką galima įsivaizduoti kaip finansinių operacijų grafą, kuris gali būti atvaizduotas kaip kryptinis svorinis grafas (5 pav.), kuriame kryptis yra finansinės operacijos kryptis (iš siuntėjo piniginės į gavėjo piniginę), o svoris yra pervedamos kriptovaliutos kiekis (vertė).



5 pav. kryptinis svorinis grafas

Ši technologija yra ir blokų grandinių, bei jomis pagrįstų kriptovaliutų pagrindas. Kriptovaliutų atveju, finansinė operacija yra iš vieno adreso į kitą siunčiamas kriptovaliutos kiekis. Šis sandoris transliuojamas į tinklą ir įtraukiamas į blokų grandinę, tuomet ji patikrinama tinklo kasėjų.

Blokų grandinių finansinių operacijų ypatybės:

- Decentralizavimas – operacijos registruojamos decentralizuotame kompiuterių tinkle o ne valdomame vieno subjekto (įmonės ar organizacijos).
- Nekintamumas – į tinklą įrašyta finansinė operacija negali būti pakeičiama ar ištrinta, dėl to suklastoti istoriją tampa beveik neįmanoma.
- Skaidrumas – visos finansinės operacijos matomos visam tinklui, tai padeda užtikrinti, kad šios yra tinkamai naudojamos.
- Saugumas – finansinės operacijos apsaugotos naudojant kriptografinius metodus, todėl neautorizuotoms šalims tampa sunku jas pasiekti ar pakeisti.

1.11. Kriptovaliutų finansinių operacijų auditas

Kaip ir kiti finansiniai instrumentai apimantys pinigų plovimo bei nusikaltimų prevenciją, kriptovaliutų auditas yra procesas kuris apima kriptovaliutų finansinių operacijų analizę ir įvertinimą. Tai yra svarbus finansinės apskaitos aspektas.

Šiais laikais, kuomet kriptovaliutos vis labiau integruojamos į verslą, daugiau žmonių yra įtraukiami į jų investavimą, natūraliai iškyla poreikis ir finansinių ataskaitų, kurios nurodo asmens kriptovaliutų

veiklą. Svarbu tai, kad prieš tai išvardytos savybės padaro blokų grandinių technologiją nesunkiai audituojamą. Reikėtų nepamiršti, kad blokų grandinių ir kriptovaliutų technologija yra dar nauja ir ataskaitoms ar atliekamiems auditams tarptautinių standartų nėra sukurta, visgi tokios organizacijos kaip viešosios akcinės bendrovės apskaitos priežiūros taryba (angl. *Public Company Accounting Oversight Board (PCAOB)),* Amerikos sertifikuotų buhalterių institutas (angl. *the American Institute of Certified Public Accountants (AICPA)),* Atestuoti profesionalūs Kanados buhalteriai (angl. *Chartered Professional Accountants Canada (CPA Canada)),* ir Kanados viešosios atskaitomybės taryba (angl. *Canadian Public Accountability Board (CPAB))* yra sukūrusios gaires nurodančias kaip jų nuomone reikėtų teisingai atlikti finansinių operacijų analizę konkrečiam subjektui[12].

Atliekant kriptovaliutų finansinių operacijų auditą atliekami keli veiksmai:

- Gaunamos tiriamo subjekto finansinės operacijos, dokumentai bei kiti susiję įrašai. Šie dokumentai apima operacijų įrašų išrašus, piniginių adresus bei bet kokie kiti svarbūs dokumentai.
- Tikrinamas finansinių operacijų teisėtumas ir tikslumas.
- Likučių sutikrinimas. Tai apima apskaitos įrašų sulyginimą su blokų grandinių įrašytų finansinių operacijų likučiais ir neatitikimų nustatymą.
- Įstatymų laikymosi patikrinimas. Šiuo patikrinimu siekiama nustatyti, ar atliekant kriptovaliutų operacijas nebuvo pažeisti šalyje galiojantys įstatymai ir reglamentai, tokie kaip pinigų plovimo ir sukčiavimo prevencijos.
- Surenkamos ir pateikiamos ataskaitos išvados.

Atliktas auditas gali padėti aptikti sukčiavimo atvejus: kriptovaliutų auditas gali padėti aptikti nesąžiningas ar neteisėtas operacijas, o tai gali padėti išvengti finansinių nuostolių ir apsisaugoti nuo elektroninių nusikaltimų. Toliau gilinti žinias nelegalių finansinių operacijų aptikime siūlo ir Kinijos mokslininkų 2021 metais sukurtas straipsnis[32]. Įmonėms atlikus kriptovaliutų auditą taip pat sustiprėja investuotojų pasitikėjimas, nes taip užtikrinama, kad įmonės finansinės ataskaitos yra tikslios ir patikimos.

1.12. Nelegalių finansinių operacijų aptikimas kriptovaliutų sistemose

Augant kriptovaliutų populiarumui, jų naudojimas išaugo ir tarp nusikaltėlių. Kriptovaliutos yra tinkama terpė nelegaliems atsiskaitymams dėl šių priežasčių[28]:

- Pseudoanonimiškumas - kriptovaliutos gali pasiūlyti didelį anonimiškumo laipsnį, todėl gali būti sunku atsekti įvykdytas finansines operacijas iki jų pradinio šaltinio. Nusikaltėliai naudojasi šia savybe, kad išvengtų aptikimo.
- Decentralizuotų tinklų reguliavimo trūkumas. Kadangi kriptovaliutas yra sunku reguliuoti, skirtingai nei tradicines finansines sistemas, nusikaltėliai kriptovaliutų tinkluose dažnai net nebandomi aptikti.
- Sudėtingumas – teisėsaugoms institucijoms net ir aptikus nelegalius sandorius gali būti sunku įrodyti kaltę, nes tokius nusikaltimus pakankamai sunku tirti, reikalinga didelė patirtis ir ištekliai.

Šiomis savybėmis pasinaudoję nusikaltėliai atlieka neteisėtas finansines operacijas kriptovaliutų tinklo viduje. Dažniausiai nusikaltėliai piktnaudžiauja kriptovaliutomis[19]:

- Plaudami pinigus. Taip nusikaltėliai stengiasi išplauti savo nelegalių veiklų pajamas.
- Sukčiaudami. Nusikaltėliai gali bandyti įtikinti asmenis siųsti kriptovaliutas jiems, naudodami vienokias ar kitokias technikas.
- Vagystėms. *Bitcoin* ir dauguma kitų piniginių tėra simbolių seka (privatūs raktai), nusikaltėliai dažnai bando perimti kompiuterių prieigą ir gauti šiuos raktus.
- Atlikdami tamsiojo interneto sandorius. Tamsusis internetas yra vieta kur parduodamos ir perkamos nelegalios prekės ir paslaugos, atsiskaitymams dažniausiai naudojamos kriptovaliutos.

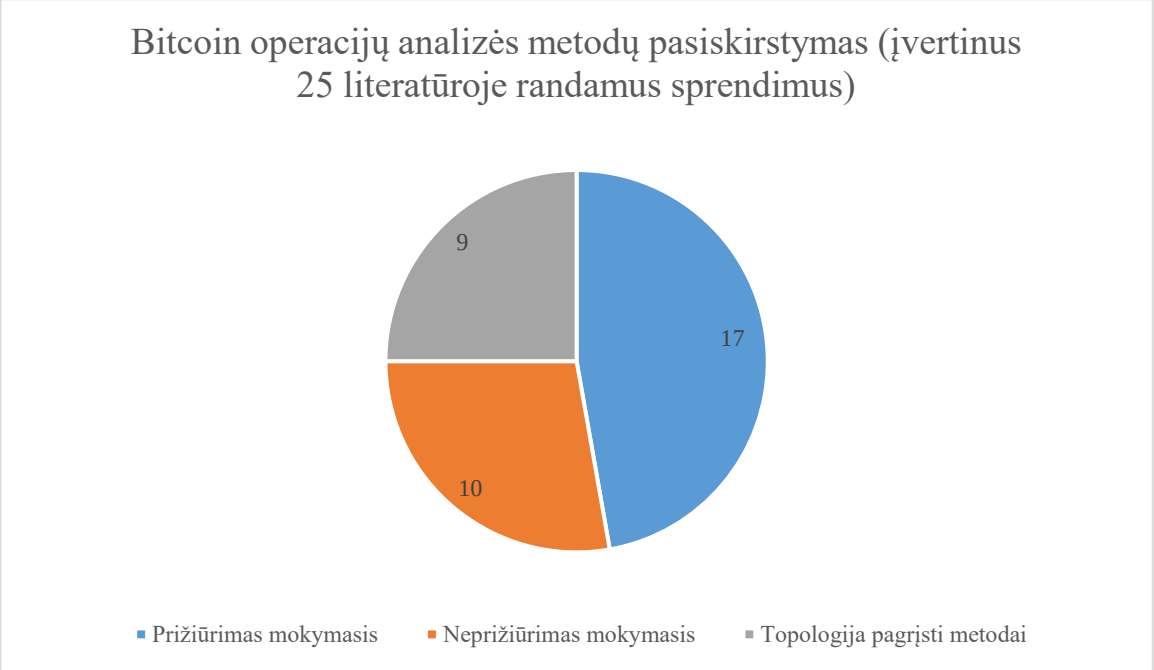
1.13. Mašininio mokymosi naudojimas aptinkant nelegalias finansines operacijas

Nėra lengvo būdo nustatyti, ar finansinė operacija yra legali ar ne. Visgi yra keletas ženklų, kurie gali sufleruoti, kad atlikta operacija yra įtartina:

- Vienas iš operacijos adresų yra žinomas didelės rizikos adresas.
- Įtartini operacijų dėsningumai – itin dideli pervedamos valiutos kiekiai, dažni periodiniai pervedimai gali sufleruoti apie tai, jog finansinė operacija atliekama nusikalstamiems tikslams.

Šiuos dėsningumus pastebėti žmogaus akiai yra itin sunku, todėl tam yra pasitelkiamas mašininis mokymasis. Pažangių mašininio mokymosi algoritmų taikymas veiksmingai kriptovaliutų rinkos priežiūrai yra svarbi būsimų šios srities tyrimų kryptis[26].

Mašininis mokymasis yra vienas svarbiausių kriptovaliutų tyrimo įrankių. Tam, kad aptikti neteisėtas operacijas kriptovaliutų sistemose, yra privaloma atlikti finansinių operacijų analizę. Šiai analizei atlikti beveik visada naudojami mašininio mokymosi metodai[19].



6 pav. *Bitcoin* operacijų analizės metodai

Mašininio mokymosi algoritmai užima didžiąją dalį visų operacijų analizės metodų (6 pav.).

Įmonės *Elliptic*, užsiimančios blokų grandinių analize, atstovai 2019 metais kartu su *IBM* tyrėjais padarė didžiulį proveržį nelegalių finansinių operacijų aptikimo srityje[31]. Jie išleido didžiulį duomenų rinkinį, kuris sudarytas iš *Bitcoin* finansinių operacijų, kurios klasifikuotos pagal tai ar tos finansinės operacijos tikslas išplauti pinigus ar ne. Pasinaudodami šiais duomenimis grupė tyrėjų išleido tyrimą, kuriame aprašė savo bandymus pritaikyti mašininį mokymąsi, problemai spręsti[21].

1.14. Privatumo pažeidimai kriptovaliutų tinkluose

Kriptovaliutų anonimiškumas nėra absoliutus, dažnu atveju analizuojant didelius kiekius duomenų įmanoma deanonimizuoti vartotojus – taip yra todėl kad dauguma blokų grandinių yra viešos. Technikos naudojamos finansinių operacijų dalyvių atskleidimui:

- Atvirų duomenų analizė. Sujungus piniginės adresą su asmeniniais duomenimis galima nustatyti tikruosius tinklo finansinių operacijų dalyvius. Tai gali atsitikti nutekėjus kriptovaliutų keityklų duomenims, kadangi jos neretai prašo patvirtinti savo asmeninius duomenis dėl pinigų plovimo prevencijos, duomenys gali būti atskleisti socialiniuose tinkluose.

- Laiko analizė. Analizuojant finansinių operacijų grandines piniginėje galima juos susieti su konkrečiais piniginės naudotojo įpročiais – paros laiku kuomet daromas finansinės operacijos, siekiama koreliuoti pinigų srautus su vieša informacija, pavyzdžiui pranešimais socialiniuose tinkluose.

- Adresų analizė. Šios technikos metu analizuojama kaip piniginės sąveikauja tarpusavyje, pavyzdžiui jeigu kelios skirtingos piniginės siunčia lėšas į naują piniginę, tikėtina, kad jos priklauso tam pačiam asmeniui arba asmenys kuriems priklauso piniginės yra tarpusavyje susiję ne tik skaitmeniniame pasaulyje.

- Dulkių atakos. Technika, kuomet į didelį piniginių skaičių siunčiamos mažytės kriptovaliutų sumos (dulkės). Toliau atakuojantis asmuo stebi kaip dulkės yra naudojamos – kai piniginės savininkas atlieka naują finansinę operaciją, dažnai sujungia nepastebėtas dulkes su jau turimomis sumomis, taip stengiamasi susieti pažymėtus adresus su kitais adresais[1].

Siekiant išgauti didesnį anonimiškumo laipsnį, kriptovaliutų blokų grandinių naudotojai gali imtis keletos veiksmų:

- Naujų piniginių generavimas. Vietoj daugkartinio piniginės naudojimo, kas kurį laiką galima keisti piniginės adresus, tai apsunkina galimybę susieti skirtingas pinigines su vienu asmeniu.
- Decentralizuotos keityklos. Jos leidžia prekiauti kriptovaliutomis be būtinybės atskleisti savo asmeninius duomenis centralizuotai institucijai.
- Maišytuvai. Egzistuoja tokia paslauga, kurios metu naudotojo finansinės operacijos yra sumaišomos su kitų visiškai nepažįstamų asmenų lėšų pervedimais.

Visgi, naudojant šias technikas didėja ir apgavystės rizika, nes naudojantis mažiau žinamomis paslaugomis galima tapti auka. Taip pat kai kurie veiksmai, skirti anonimiškumui didinti teisiniuose procesuose gali būti traktuojami kaip bandymas nuslėpti veiklą.

1.15. Kriptoturto teisinė bazė ir reguliavimas

Teisinė bazė ir reguliavimas kriptovaliutų sferoje yra labai dinamiška, nuolat kintanti sritis. Pagrindinės tendencijos pasaulyje yra susijusios su didesnio reguliavimo bei didesnio tarptautinio bendradarbiavimo poreikiu – vis daugiau šalių pripažįsta, kad reikalingi aiškūs nurodymai, siekiantys apsaugoti investuotojus, o to įgyvendinimas reikalauja globalaus požiūrio į šias problemas.

Europos sąjungos lygmeniu šiuo metu yra aktyviai diegiamas kriptoturto reglamentas, kuris apima šiuos aspektus:

- Kriptoturto apibrėžimas, kategorijos, klasifikavimas.
- Reikalavimai kriptoturto paslaugų teikėjams.
- Kriptoturto priežiūros kontrolės mechanizmai.

Kitos pasaulio šalys:

- JAV: nėra aiškaus reguliavimo federaliniu lygmeniu, direktyvos susijusios su kriptovaliutomis leidžiamos kelių organizacijų, kurios į kriptoturtą žiūri per savo prizmę. Vidaus pajamų tarnyba nustato kokie mokesčiai turėtų būti mokami valstybei už gautas pajamas kriptoturto forma, vertybinių popierių biržos komisija nori kriptoturtą priskirti vertybiniams popieriams, reikalauja kad bet kokios kriptoturto finansinės operacijos būtų oficialiai įregistruotos.
- Kinija: griežta pozicija, draudžianti didžiąją dalį kriptovaliutų veiklos, įskaitant prekybą ir kasimą.

Kai kurios mažesnės Azijos valstybės siekia tapti kriptovaliutų centrais, kitur teisinė ir kriptoturto reguliavimo stadija yra labai ankstyva, visgi nepaneigiama, kad kriptoturtas tampa aktualia tema reikalaujančia teisinės bazės ir reguliavimo.

1.16. Kriptoturto skaitmeninė kriminalistika Lietuvoje

Lietuva neatsilieka nuo Europos Sąjungos – derina savo nacionalinę teisę su ES direktyvomis. Nagrinėjant kriptoturto nusikaltimus ekspertinius tyrimus atlieka ir prižiūri Lietuvos teismo ekspertizės centras (LTEC). Tyrimai atliekami vadovaujantis Lietuvos Respublikos įstatymine baze – baudžiamojo proceso kodeksu, civilinio proceso kodeksu, administracinių bylų teisenos įstatymu, administracinių nusižengimų kodeksu ir kitais. Tyrimų tikslas – nustatyti tiriamam įvykiui reikšmingą įrodomąją informaciją apie kompiuterinę įrangą, atkurti ar surasti duomenis susijusius su tiriamu įvykiu, nustatyti stacionarios kompiuterinės ar programinės įrangos vaidmenį tyrimo atveju[22].

2 lentelė. Informacinių technologijų ekspertiniai tyrimai Lietuvoje

Ekspertinių tyrimų rūšis	**Eilė**	**Vidutinė tyrimo atlikimo trukmė, kal. d.**
Informacinių technologijų	iki 5 mėn.(mobiliųjų įrenginių iki 2 mėn.)	75 (mobiliųjų įrenginių - 12)

Pagal pateiktą informaciją, informacinių technologijų ekspertiniai tyrimai vidutiniškai vyksta 75 kalendorines dienas, išskyrus mobiliųjų įrenginių, kurių tyrimas vykdomas 12 kalendorinių dienų (2 lentelė.).

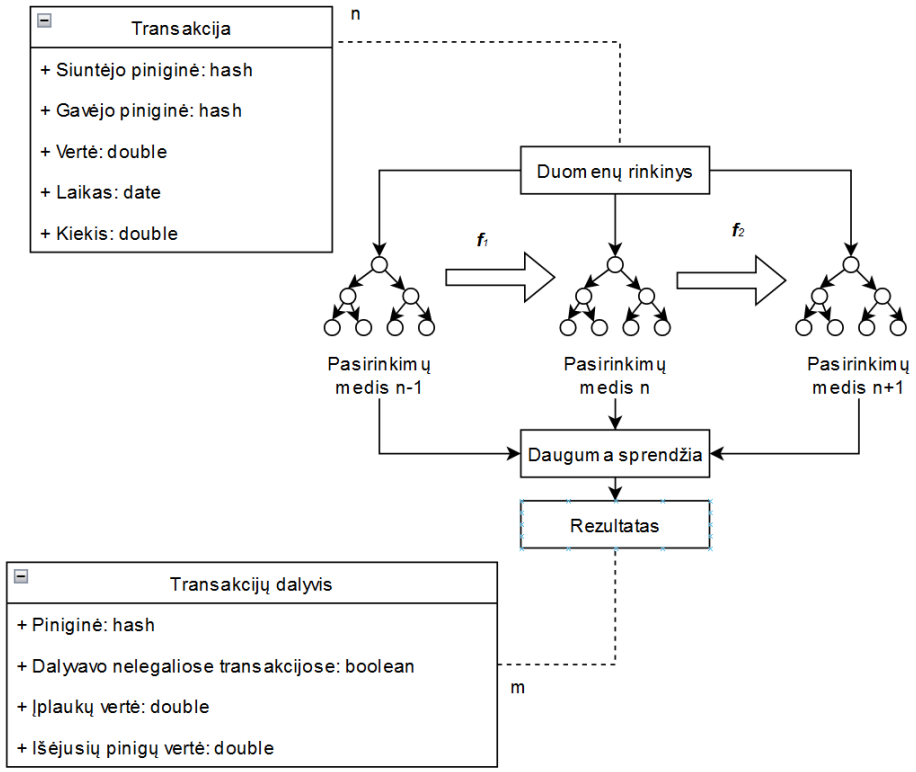
2. Tyrimo metodai ir metodika

2.1. Problema

2019 metais atliktas tyrimas nustatė, kad apie 76 milijardai dolerių vertės finansinių operacijų yra atliekamos nusikalstamiems tikslams, tai yra apie 46% visų lėšų pervedimų atliekamų *bitcoin* tinkle, šiose finansinėse operacijose dalyvauja net ketvirtis visų *bitcoin* piniginių[9]. Visgi, *bitcoin*, kaip ir kiekvienos kitos finansinės ekosistemos, reguliavimo klausimas yra kontraversiškas. Iš vienos pusės, finansinis reguliavimas gali suteikti sistemai stabilumo, bei saugumo, užkirsti kelią nelegalioms veikloms, mažinti riziką, iš kitos pusės didesnis kontroliavimas sumažina privatumą, netinkamai valdant renkami duomenys gali būti panaudoti neteisėtiems tikslams, taip pat augant kontrolės lygmeniui, didėja ir biurokratizmas, tai gali stabdyti finansinį efektyvumą (pvz. finansinių operacijų greitį). Nei vienas kraštutinumas nėra teisingas, kiekviena sistema turi turėti kontrolę tačiau tai neturi riboti žmonių laisvės.

2.2. Siūlomas sprendimas

Šiuo metu *bitcoin* reguliavimas yra minimalus, šio darbo tikslas yra panaudoti mašininio mokymosi algoritmus nelegalių kriptovaliutų finansinių operacijų aptikimui, sukurti algoritmą gebantį paaiškinti savo sprendimus, sukurtą metodiką panaudoti patariamojo karkaso sukūrimui, kurio paskirtis – padėti finansinių nusikaltimų tyrėjams nustatyti finansinių operacijų legalumą, pateikti analitinius duomenis apie pervedimų grandines vedančias į piniginę (7 pav.).



7 pav. Siūlomo sprendimo schemos eskizas

Patariamojo karkaso sukūrimui pasiekti, reikia įgyvendinti šiuos žingsnius:

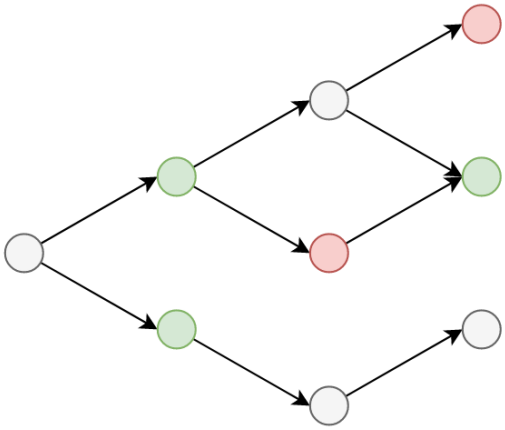
1. Duomenų apdorojimas (paruošimas mašininio mokymosi metodams)
2. Modelių treniravimas, lyginimas tinkamiausio parinkimas

3. Modelio sprendimų paaiškinamumo įgyvendinimas
4. Patariamojo karkaso sukūrimas naudojantis ištreniruotu modeliu

2.2.1. Duomenų apdorojimas

Modelio treniravimui pasirinkta naudoti viešą duomenų rinkinį, kurį paskelbė *Elliptic kaggle* duomenų talpykloje[8]. Šis anoniminis duomenų rinkinys sudarytas iš *bitcoin* finansinių operacijų surinktų iš *bitcoin* blokų grandinės. Mazgas šiame grafike simbolizuoja pinigų pervedimą, o kraštinė suprantama kaip srautas iš vienos finansinės operacijos į kitą (8 pav.). Kiekvienas mazgas turi 166 laukus ir teisėtumą nurodančią klasę, kuri gali įgauti sekančias reikšmes:

- Teisėta (42019 stebinių arba 21% visų finansinių operacijų)
- Neteisėta (4545 stebiniai arba 2% visų finansinių operacijų)
- Nežinoma (likusios finansinės operacijos)



8 pav. *Elliptic* duomenų rinkinio struktūra

Duomenys sudaryti iš 49 laiko periodų, kurie sudaryti iš 3 valandų. Šie blokai savyje turi finansines operacijas įvykdytas konkrečiame laiko tarpe. Nėra finansinių operacijų jungiančių skirtingus laiko periodus. Kiekvienas stebinys turi 166 laukus, iš kurių:

- Pirmieji 94 laukai nurodo bendrąją informaciją apie finansinę operaciją (pvz. operacijos atlikimo laikas, pervedimo mokestis, siunčiamo BTC kiekis ir t.t)
- Kiti 72 laukai yra išvesti, gauti apskaičiuojant maksimumus, minimumus tarp gretimų operacijų, standartinį nuokrypį, koreliacijos koeficientus.

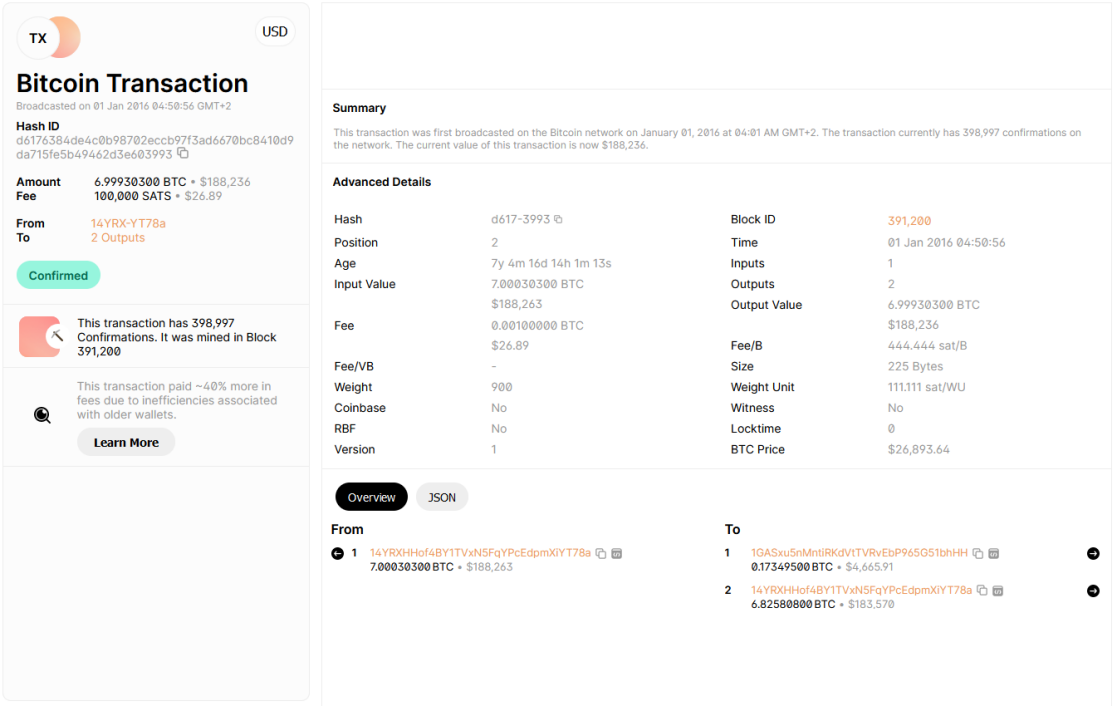
Sukurti patariamąjį karkasą su anoniminiais duomenimis ištreniruotu modeliu beveik neįmanoma, todėl apdorojant duomenis bus naudojamas dar vienas duomenų rinkinys – duomenų rinkinys atskleidžiantis *Elliptic* anoniminių finansinių operacijų identifikatorius (angl. *hash*) (3 lentelė.)[6].

3 lentelė. Atskleistos Elliptic duomenų rinkinio finansinės operacijos

txId	transaction
230325127	d6176384de4c0b98702eccb97f3ad6670bc8410d9da715fe5b49462d3e603993
230325139	300c7e7bb34263eae7ff8b0a726d5869bf73d71081490c45a9536a31560f1fd7
86875675	7c790a31090462d720a172b3f55a51af2514971070db6686e337ccc486840dcd

Šis duomenų rinkinys atskleidžią 99,5% visų finansinių operacijų – *txId* yra anonimizuotas operacijos identifikatorius, o *transaction* stulpelis atskleidžia tikrą operacijos ID.

Į *blockchain.com* puslapį įvedus finansinės operacijos ID, galima pamatyti pilną informaciją susijusią su finansine operacija (9 pav.).



9 pav. Informacija apie BTC finansinę operaciją[34]

Šis, kaip ir dauguma puslapių turi viešus programavimo sąsajos taškus (angl. *API*), kuriais pasinaudojus galima gauti duomenis apie kiekvieną atskleistą anoniminę finansinę operaciją (10 pav.). Taigi sujungus anonimizuotą klasifikuotą duomenų rinkinį su duomenimis gautais naudojant išorinę programavimo sąsają, gaunamas klasifikuotas duomenų rinkinys.

GET `https://blockchain.info/block/000000000000000000a7b4999c723ed9f308425708577c76827ade51062e135a?format=json`

```
{
    "block_hash": "00000000000000002e3354f741cf0a3b8976c660431980cacfc04bac26ea9f5",
    "block_height": 391200,
    "block_index": 2,
    "hash": "d6176384de4c0b98702eccb97f3ad6670bc8410d9da715fe5b49462d3e603993",
    "addresses": [
        "14YRXHHof4BY1TVxN5FqYPcEdpmXiYT78a",
        "1GASxu5nMntiRKdVtTVRvEbP965G51bhHH"
    ],
    "total": 699938300,
    "fees": 100000,
    "size": 225,
    "vsize": 225,
    "preference": "high",
    "confirmed": "2016-01-01T02:50:56Z",
    "received": "2016-01-01T02:50:56Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 2,
    "confirmations": 402858,
    "confidence": 1,
    "inputs": [
        {
            "prev_hash": "123324c379b4e98c2b0633012f95145d88ab301d39edc911c0cd1a1eef7b96e8",
            "output_index": 0,
            "script":
                "47304402201a263c71f3e78557d79d99433003ce7ab42e8466eebbec28583381e1d27238860220438211911bf565288257a916258756ce9438a04d74c5f0d0e4f4158d2e830ec0012103c5bd73b923f163b6427a6e39dc2ef
                1d01dc76a7e007d608626802f4a8b3ad64a",
            "output_value": 700038300,
            "sequence": 4294967295,
            "addresses": [
                "14YRXHHof4BY1TVxN5FqYPcEdpmXiYT78a"
```


10 pav. Duomenys apie finansinę operaciją gauti naudojant programavimo sąsają

Duomenys gauti naudojant programavimo sąsają išsaugomi *JSON* formatu. Toliau gauti duomenys sujungiami pagal schemą (11 pav.).

11 pav. Duomenų rinkinio kūrimo schema

Galima matyti visus naujai kuriamo duomenų rinkinio komponentus ir kaip šie susiję. Taip gaunamas duomenų rinkinys, kurio stebiniai turi šiuos požymius:

- Atskleistas finansinės operacijos identifikatorius
- Legalumą nurodanti etiketė gauta iš anonimizuoto *Elliptic* duomenų rinkinio.
- Požymiai gauti iš *blockchain.info* programavimo sąsajos (įvesčių skaičius, mokestis, laikas ir t.t.)

Reikėtų atkreipti dėmesį, kad naudojant skirtingas finansines operacijas treniravimui duomenų rinkinys turės skirtingą požymių skaičių, taip nutinka todėl, kad kiekvienos finansinės operacijos duomenys gauti iš išorinės programavimo sąsajos gali turėti skirtingą požymių skaičių, priklausomai nuo to kiek ji turi įvesčių ir išvesčių.

2.2.2. Modelių treniravimas

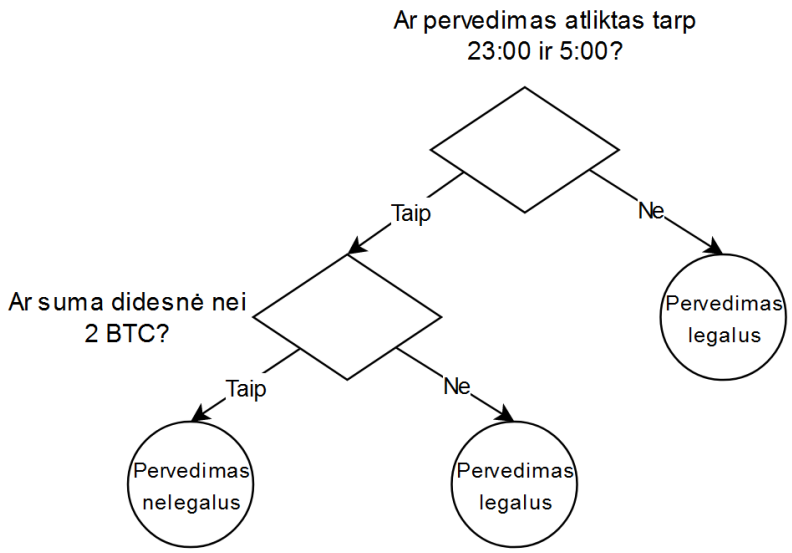
Paruošus duomenis atliekamas modelių apmokymas (treniravimas). Jis bus atliekamas naudojant naujai sukurtą duomenų rinkinį, bus vertinamas ištreniruotų modelių tikslumas, treniravimo greitis, paaiškinamumas.

2.2.3. Modeliai

Klasifikavimo uždaviniui spręsti buvo pasirinkti 3 modeliai: Atsitiktinis miškas, *XGBoost*, *ADABoost*.

Atsitiktinis miškas

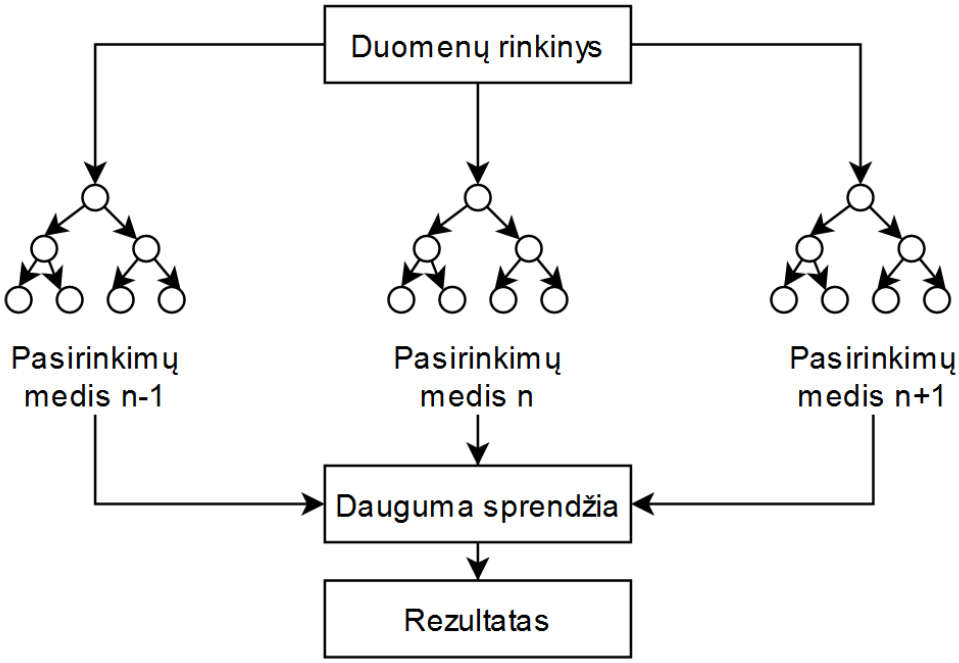
Atsitiktinis miškas – vienas iš populiariausių mašininio mokymosi algoritmų, dažniausiai naudojamas atliekant klasifikavimo ir regresijos uždavinius. Norint suprasti kas yra atsitiktinis miškas, pirmiausia reikėtų suprasti kas yra sprendimų medis. Sprendimų medis, tai modelis sudarytas iš mazgų, kurių kiekvienas tarsi kelia klausimą, ir turi 2 išsišakojimus, vienas pasirenkamas kai sąlyga tenkinama, kitas kai netenkinama. 12 pav. galima matyti kaip galėtų atrodyti supaprastintas BTC operacijų klasifikavimo medis.



12 pav. BTC operacijas klasifikuojančio sprendimų medžio pavyzdys

Šis medis gautų finansinės operacijos duomenis, tikrintų kada finansinė operacija atlikta, jeigu ji atlikta naktį, tikrintų ar pervesta suma yra didesnė nei 2 BTC. Ištreniruotas sprendimų medis gali turėti šimtus mazgų, visgi kuo daugiau mazgų, tuo didesnė tikimybė, kad medis persimokė.

Atsitiktinis miškas yra modelis sudarytas iš daugybės sprendimų medžių – miškui padavus finansinę operaciją, jis ją perduos kiekvienam sprendimų medžiui, visi medžiai atliks savo klasės sprendimą, tuomet modelis pagal tai kurią klasę spėjo daugiau sprendimų medžių parinks klasę (13 pav.).

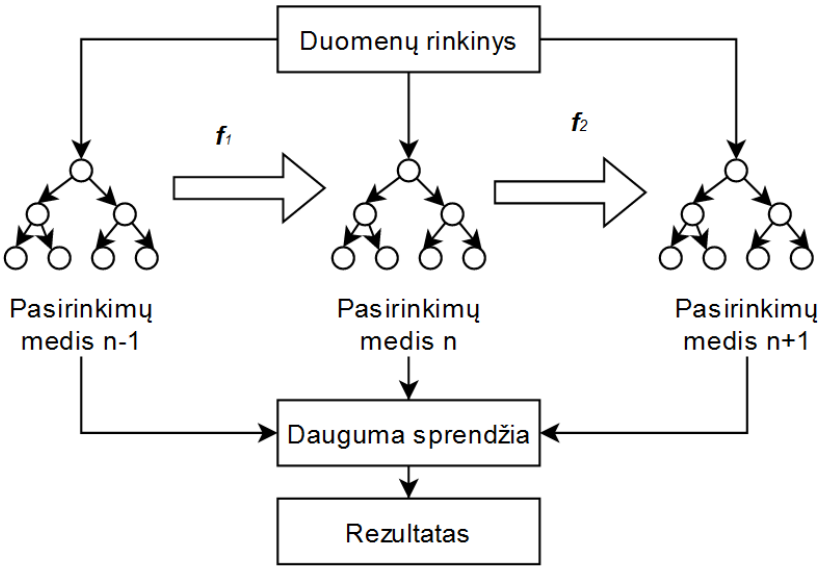


13 pav. Atsitiktinio miško sprendimų priėmimo schema

Atsitiktinis miškas sumažina modelio persimokymą – kadangi sprendimui priimti naudojamas ne vienas medis tai ženkliai didina modelio abstraktumą, tai reiškia modelis neblogai apsimoko ir su grubiomis išskirtimis. Atsitiktinio miško apmokymo laikas yra trumpas (lyginant su kitais mašininio mokymosi algoritmais). Visgi paaiškinti kodėl atsitiktinis miškas priėmė vienokį ar kitokį sprendimą yra ne taip paprasta – tenka atskirai nagrinėti kiekvieną sprendimų medį.

XGBoost

XGBoost (angl. *eXtreme Gradient Boosting*) – vienas iš prižiūrimojo mašininio mokymosi modelių. Šis modelis skiriasi nuo atsitiktinio miško tuo, kad sprendimų medžiai yra treniruojami paeiliui, kiekvieną kartą tobulinant (angl. *boosting*) modelį, ištaisant prieš tai buvusio modelio (sprendimų medžio) klaidas (14 pav.). Paskui kaip ir atsitiktinio miško modelyje, visi sukurti modeliai balsuoja, tačiau šį kartą modeliai gali turėti skirtingus sprendimo svorius.

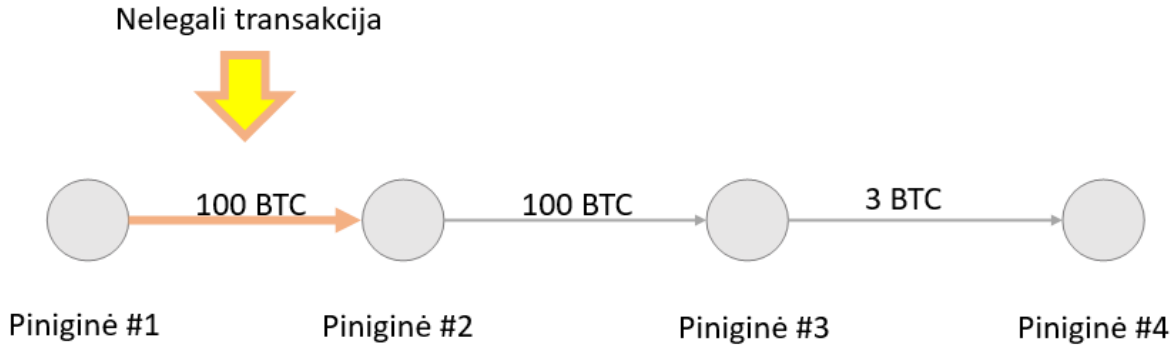


14 pav. *XGBoost* sprendimo priėmimo schema

Visų pirma apmokomas sprendimo medis *n-1*, tuomet modelis patikrina kaip gerai šis medis klasifikuoja, išsaugo medžio struktūrą, lapams priskiria svorius. Toliau su šiomis žiniomis treniruojamas medis *n*. Šis procesas kartojamas iki nurodyto medžių skaičiaus parametro. *XGBoost* dažniausiai yra greičiau ištreniruojamas ir greičiau sprendimus priimantis modelis lyginant su atsitiktiniu mišku. Šis modelis taip pat analitikui suteikia daugiau konfigūravimo galimybių, kadangi kiekvienoje iteracijoje pritaikoma nuostolių funkcija gali būti pritaikyta pagal poreikius. *XGBoost* modelį yra dar sunkiau interpretuoti, taip pat jis yra labiau linkęs persimokyti, yra jautrus išskirtims bei duomenų trūkumams.

2.2.4. Nelegalių finansinių operacijų radimo uždavinys

Pasirinkti modeliai atlieka išsamią *Bitcoin* tinklo finansinių pervedimų duomenų analizę - ieško įtartinų šablonų ir anomalijų (15 pav.).



15 pav. Nelegalių lėšų pervedimų radimo uždavinys

Nelegalių lėšų pervedimų aptikimo uždavinio sprendimą gali apsunkinti šios aplinkybės:

- Ribotas kiekis patikimai pažymėtų duomenų. Tiksliai sužymėti finansinių operacijų duomenis yra itin sudėtinga, ir gali užimti daug laiko bei resursų, visgi internete yra viešų duomenų

rinkinių kurie yra atlikę šį sudėtingą darbą. Surinkti duomenis ir sužymėti galėtų padėti tokie įrankiai kaip *chainabuse*, kurie kaupia duomenis apie viešai paskelbtas nelegalias pinigines bei finansines operacijas įvairiose blokų grandinėse.

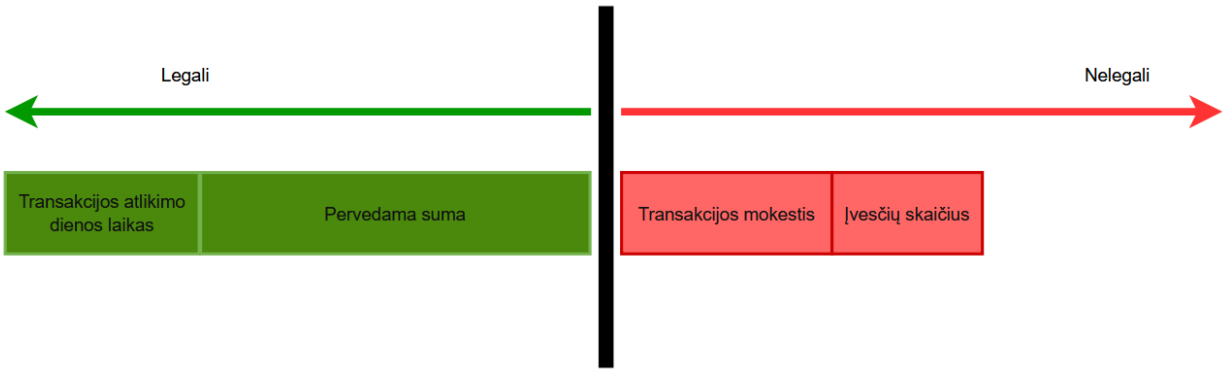
- Nelegalių finansinių operacijų įvairovė ir naujų maskavimo metodų atsiradimas – nelegalios veiklos vykdytojai nuolat tobulėja, keičia savo taktikas, naudoja šiuolaikiškus metodus, siekdami užmaskuoti savo pinigų srautus, taip, kad šie niekuo neišsiskirtų.

- Informacijos dalijimosi trūkumas. Piktavaliai dažnai veikia ne per vieną instituciją, naudoja ne vieną piniginę, kurios nebūtinai egzistuoja tame pačiame kriptovaliutos tinkle. Tokio tipo informacijos dalijimasis tarp institucijų renkančių duomenis gali būti ribotas, o tai apsunkina nelegalių veiklų aptikimą.

Norint sėkmingai sukurti nelegalių finansinių operacijų aptikimo modelį reikia kruopščiai apgalvoti šiuos iššūkius bei ieškoti tinkamų sprendimų.

2.2.5. Modelio sprendimo paaiškinimas

Naudojant sudėtingus modelius gali būti sunku suprasti, kas lėmė vienokį ar kitokį modelio sprendimą. Modeliui aiškinti bus pasitelkta *SHAP* analizė. Ši analizė atliekama po modelio sprendimo ir gali tiksliai parodyti kokie modelio požymiai buvo svarbiausi priimant konkretų sprendimą, kadangi prognozuojama klasė yra dvireikšmė (finansinė operacija yra legali arba ne).



16 pav. *SHAP* dvireikšmės analizės vizualizacijos prototipas

16 pav. galima matyti, kaip galėtų atrodyti *SHAP* požymių prisidėjusių prie finansinės operacijos klasifikavimo vizualizacija. Kiekvienas požymis, kuriuo buvo remtasi atliekant prognozę atvaizduojamas legalioje arba nelegalioje pusėje, priklausomai šis prisidėjo prie klasifikavimo. Taip pat čia svarbus ir požymio indėlis, kuo jis didesnis, tuo didesnis požymio dedamosios dalies plotas. 16 pav. pavyzdį reiktų interpretuoti taip: Pervedama suma ir operacijos atlikimo dienos laikas modeliui indikavo, kad finansinė operacija yra legali, tuo tarpu operacijos mokestis ir įvesčių skaičius indikavo, kad finansinė operacija nelegali. Kadangi legalioji pusė užima didesnį plotą, modelis priėmė sprendimą, kad finansinė operacija legali.

Iššūkiai kylantys atliekant *SHAP* analizę:

- Priklausomi požymiai. *SHAP* metodas gali susidurti su sunkumais interpretuojant požymių indėlius, kuomet jie tarpusavyje stipriai koreliuoti.

- Atskaitos taško parinkimas. *SHAP* reikšmės apskaičiuojamos lyginant prognozę su atskaitos reikšme, o ši dažniausiai yra vidutinė visų prognozių reikšmė. Netinkamai parinktos reikšmės gali turėti įtakos modelio paaiškinimams.

- Interpretavimo sunkumai esant dideliam kiekiui požymių. *SHAP* metodo vizualizacijos gali netekti prasmės, kuomet modelio sprendimui įtaką turėjo tūkstančiai požymių, tokiu atveju jos tampa perkrautos ir sunkiai suprantamos.

Reikėtų suprasti, kad nors *SHAP* analizė ir paaiškina kaip modelis priėmė sprendimus, ji ne visada atspindi priežastinius ryšius.

2.2.6. Patariamojo karkaso sukūrimas naudojantis ištreniruotu modeliu

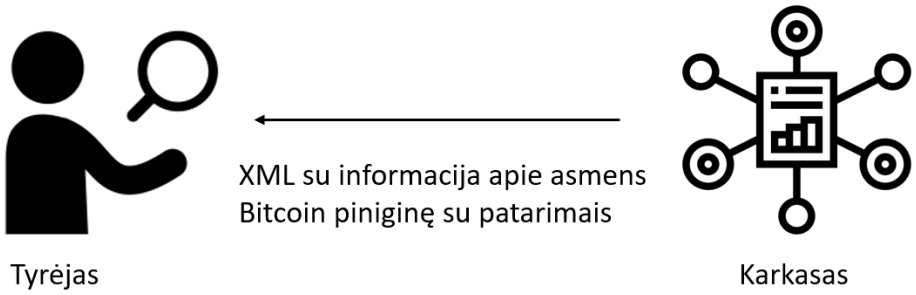
Naudojantis sukurtais modeliais, bus kuriamas patariamasis karkasas, padėsiantis finansinių nusikaltimų analitikams analizuoti *Bitcoin* tinklą. Karkasas finansinių nusikaltimų tyrėjui paprašius pateiktų finansinių operacijų susijusių su nurodyta pinigine sąrašą, taip pat pateiktų koeficientus prie operacijų, kokia tikimybė, kad finansinė operacija galimai yra naudojama nelegaliems tikslams, taip pat turėtų tokias funkcijas:

- Duomenų apdorojimas – karkasas galėtų turėti galimybes apdoroti didelį duomenų kiekį ir atlikti skirtingus duomenų filtravimo ir transformavimo veiksmus. Tai apims finansinių operacijų šaltinių filtravimą pagal tam tikrus kriterijus.

- Duomenų vizualizacija - karkasui svarbu turėti vizualizacijos įrankius, kurie padėtų analitikams geriau suprasti ir išnagrinėti duomenis. Pavyzdžiui: interaktyvūs grafikai, diagramos, anomalijų analizė ir kitos vizualizacijos technikos, kurios padėtų tyrėjams pastebėti tendencijas ir atrasti ryšius tarp finansinių operacijų.

- Mašininio mokymosi algoritmo patarimai apie piniginės dalyvavimą nelegaliose finansinėse operacijose. Reikia suprasti, kad mašininio mokymosi algoritmai irgi klysta, todėl jie gali būti tik patariamojo tipo, lyg nuorodos į kurias finansines operacijas reikėtų pasigilinti giliau.

Kuriant tokį karkasą būtų susiduriama su didelių duomenų kiekio apdorojimo problema, reikėtų apsvarstyti teisės aktus ir reguliavimus, kurie gali skirtis priklausomai nuo valstybės, kurios tyrėjai naudotų karkasą.



17 pav. Karkaso panaudojimo pavyzdys

Sistemizuoti skaitmeniniai pėdsakai galėtų būti pateikiami XML 2022 ISO ar kitu standartizuotu formatu ir naudojami kaip vertingas įrodymas teisme (17 pav.).

3. Prototipo realizacija ir rezultatų tyrimas

3.1. Prototipo realizavimo priemonės

Prototipui realizuoti pasitelktos priemonės:

- *Python 3.12.3*
- *Node.js 22.14.0*
- *React.js 18.2.0*
- *Typescript 5.1.6*
- *Python* bibliotekos: *sklearn, numpy, pandas, network, pickle, fastapi*

Parašyti *python* scenarijai (angl. *scripts*) apdoroja duomenis, sudaro naują duomenų rinkinį, apmoko mašininio mokymosi metodus, palygina juos tarpusavyje. Taip pat naudojantis biblioteka *fastapi* yra sukuriami galutiniai programavimo sąsajos taškai, į kuriuos kreipiasi naudotojo sąsaja.

3.2. Duomenų rinkinio sudarymas

Duomenų rinkinys sudarytas naudojant 2 viešai prieinamus duomenų rinkinius patalpintus svetainėje *kaggle.com*:

- *Elliptic* duomenų rinkinys[8]
- Atskleistas (deanonimizuotas) *Elliptic* duomenų rinkinys[6]

Toliau duomenys apdorojami pagal sekančius žingsnius:

- Iš *Elliptic* duomenų rinkinio išrenkamos finansinės operacijos, kurios yra suklasifikuotos kaip legalios ar nelegalios.
- Kiekvienai finansinei operacijai ieškoma atskleisto atitikmens atskleistame *Elliptic* duomenų rinkinyje.
- Identifikavus finansinę operaciją, siunčiama užklausa į *https://blockchain.info* programavimo sąsają (*API*) su prašymu gauti neapdorotą informaciją apie finansinę operaciją.
- Gauti duomenys sujungiami su *Elliptic* klasės etikete ir išsaugomi faile.

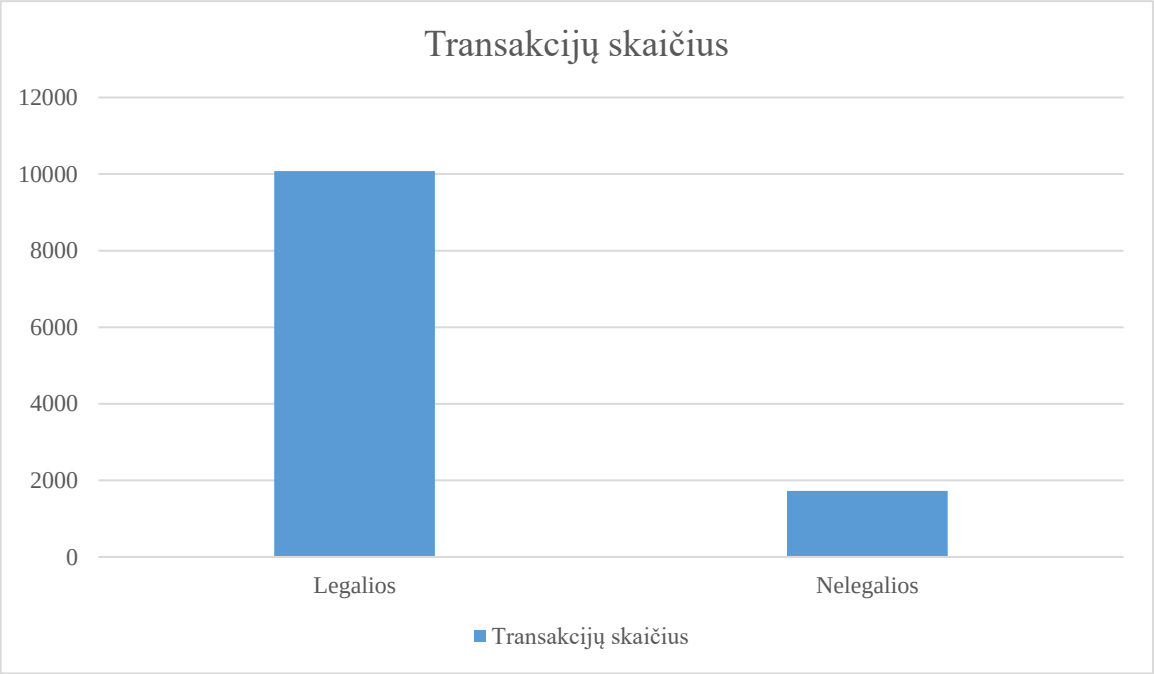
Toliau pateikiamas algoritmo pseudo-kodas:

```
klasifikuotos = []
FOR transakcija IN Elliptic_transakcijos:
  Klasifikuotos.pridėti (transakcija) jeigu transakcija suklasifikuota

klasifikuoti_tikri_id = []
FOR transakcija IN klasifikuotos:
  klasifikuoti_tikri_id.pridėti(transakcija.ID) jeigu transakcija yra atskleista
```

```
tikros_klasifikuotos_transakcijos
FOR id IN klasifikuoti_tikri_id:
   Neapdorota_transakcija = Gauti_duomenis(https://blockchain.info, id)
   Neapdorota_transakcija.Pridėti(Elliptic_etiketė)
   tikros_klasifikuotos_transakcijos.Pridėti(Neapdorota_transakcija)

Įrašyti_į_failą(tikros_klasifikuotos_transakcijos, „transakcijos.json“)
```

Gaunamas duomenų rinkinys neapdorotų atskleistų finansinių operacijų su *Elliptic* duomenų etiketėmis. Tokio duomenų rinkinio privalumas – ištreniravus mašininio mokymosi modelius su šiais duomenimis, tą patį modelį galima naudoti ir klasifikuojant realias *bitcoin* tinklo finansines operacijas.

Gautas rezultatas – beveik 12 tūkst. realių finansinių operacijų duomenų. Svarbu paminėti, jog gautas rinkinys yra stipriai išbalansuotas (18 pav.).

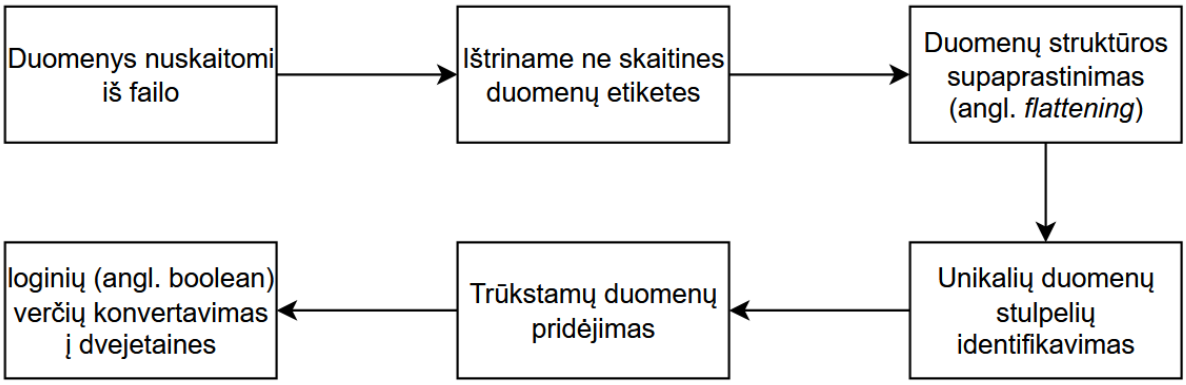


18 pav. Klasių santykis

Tam, kad šią problemą išspręsti, buvo priimtas sprendimas treniravimui naudoti tokį pat legalių finansinių operacijų skaičių kaip ir nelegalių.

3.3. Duomenų paruošimas

Duomenų paruošimas vykstą pagal 19 pav. vaizduojamą schemą.



19 pav. Duomenų paruošimas normalizavimui

Kadangi mašininio mokymosi algoritmai yra treniruojami naudojant skaitines duomenų reikšmes, kitokie stulpeliai modeliui nereikalingi todėl yra ištrinami. Duomenų struktūros supaprastinimo žingsnis transformuoja *json* formato objektų duomenis iš tokios, kelių lygių struktūros:

```
{
  "pozymis": "Pozymis 1",
  "pozymis2": {
    "pozymis3": "Pozymis 3",
    "pozymis4": "Pozymis 4"
  }
},
```

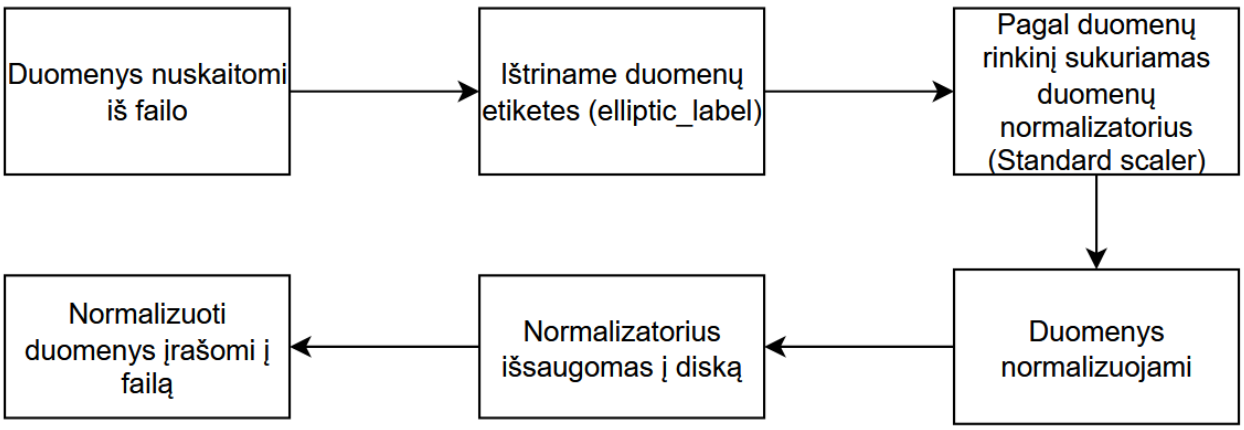
Į vieno lygio duomenų struktūrą (matricą):

```
{
  "pozymis": "Pozymis 1",
  "pozymis2_pozymis3": "Pozymis 3",
  "pozymis2_pozymis4": "Pozymis 4"
}
```

Dauguma mašininio mokymosi algoritmų yra suprojektuoti darbui su 2 ar 1 dimensijos masyvais ir tikisi nuoseklios duomenų įvesties formos. Dėl šių duomenų pobūdžio, ne visos finansinės operacijos turi visas unikalias rinkinio etiketes. Kuomet vienos iš jų trūksta algoritmas prideda numatytąją vertę, kuri konkrečiu atveju yra 0.

3.4. Duomenų normalizavimas

Toliau duomenys normalizuojami pagal 20 pav. pateiktą schemą.



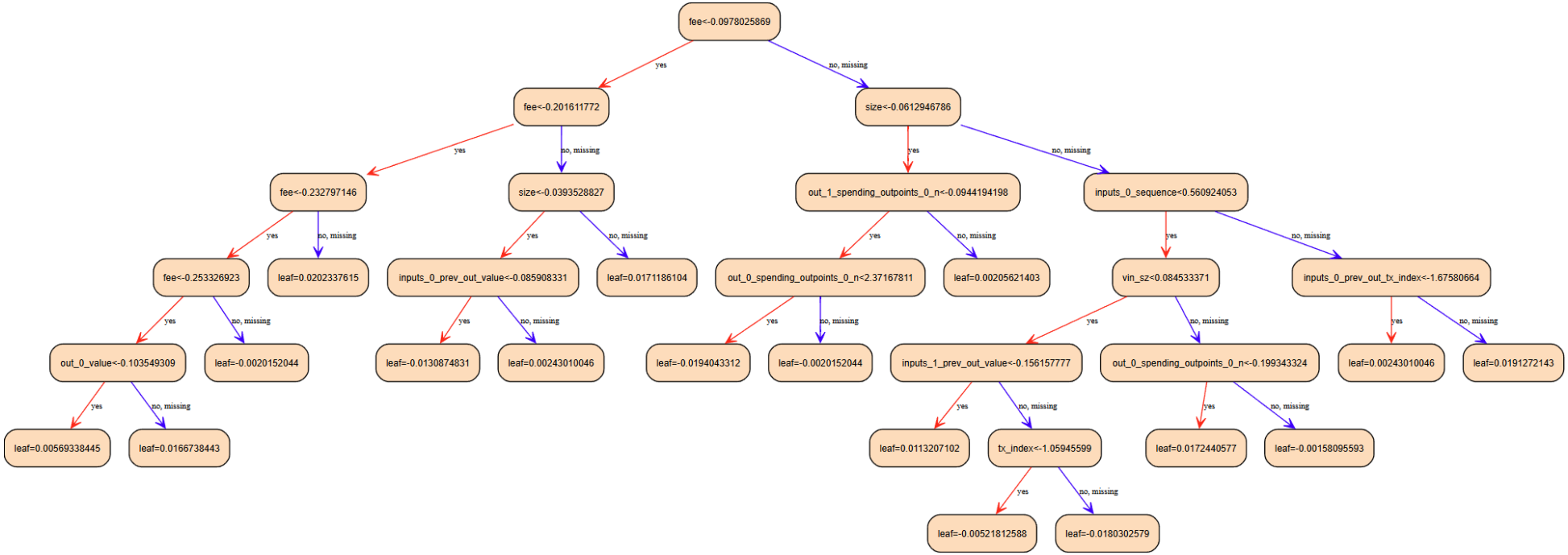
20 pav. Duomenų normalizavimas

Duomenų normalizatorius (angl. *Scaler*) keičia požymius taip, kad šie patektų į diapazoną nuo 0 iki 1. Toliau šie parametrai išsaugomi į failą naudojant *StandartScaler* objektą bei *pickle* biblioteką, tai yra labai svarbu norint turėti galimybę treniruoti modelius / prognozuoti reikšmes naudojant realaus laiko duomenis. Šis veiksmas užtikrina, kad duomenų mastelio keitimas bus taikomas vienodai ir visi požymiai išliks vienodai svarbūs modeliui.

Svarbu paminėti, kad kuriant normalizatoriaus objektą reikia laikytis principo neleidžiančio duomenims patekti iš treniravimo imties į testavimo imtį: jis turi būti apmokytas naudojant mokymosi imtį, o paskui tas pats normalizatorius turi būti naudojamas transformuoti visas imtims. Kitu atveju, jeigu jis apmokomas su visais duomenimis (testavimo ir treniravimo imtimis), jis netiesiogiai „mato“ visų duomenų statistiką – ši informacija iš esmės tampa nutekėjusia ir stipriai iškraipo galutinius rezultatus.

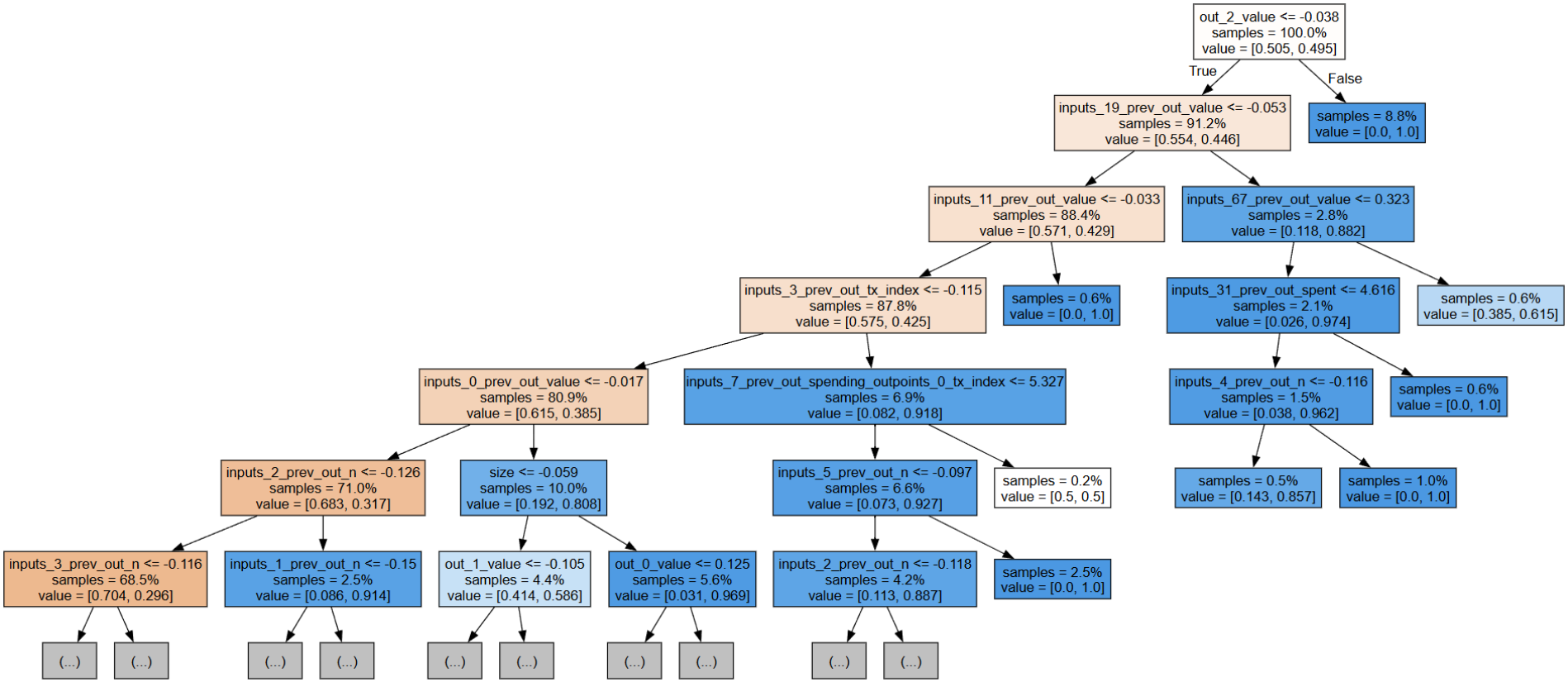
3.5. Modelių treniravimas

Paruošus duomenų rinkinį buvo treniruojami mašininio mokymosi modeliai. Pasirinkta treniruoti ir lyginti atsitiktinio miško modelį, tada naudojant skatinimo (angl. *Boosting*) strategijas gerinti modelio tikslumą bei lyginti ar modelio rezultatas gerėja ar prastėja.



21 pav. *XGBoost* algoritmo pirmasis medis

Pirmasis *XGBoost* algoritmo sukurtas sprendimų medis galėtų būti interpretuojamas tiriant bylas, kuriose reikėtų nurodyti kaip buvo priimtas sprendimas (21 pav.).



22 pav. Atsitiktinio miško pirmasis medis

Atsitiktinio miško pirmasis sprendimų medis atvaizduotas 22 pav. - lapai simbolizuoja finansinės operacijos klasę (oranžinė spalva nurodo, jog finansinė operacija yra įtartina, mėlyna –legali), išsišakojimų spalva nurodo kokia klasė yra tikėtinesnė, klasės klasifikavimui atėjus iki to mazgo.

Paveiksle atvaizduotas ne visas medis, tai yra todėl, kad šio medžio gylis yra apie 12, tai gali reikšti, kad modelis yra persimokęs, per daug prisitaikęs prie gautų duomenų ir mažai generalizuoja.

Visi ištreniruoti modeliai yra išsaugomi į failą, nes stengiamasi išvengti modelio treniravimo kiekvieną kartą kai yra poreikis atlikti klasifikavimo uždavinį.

3.6. API galutiniai taškai

Naudojant *fastAPI* biblioteką buvo sukurti 2 pagrindiniai programavimo sąsajos taškai į kuriuos kreipiasi naudotojo sąsaja:

4 lentelė. Finansinės operacijos klasifikavimo programinė sąsaja

Pavadinimas	Klasifikuoti *Bitcoin* finansinę operaciją pagal jos id
Kelias	http://127.0.0.1:8000/transaction/?txHash={txHash}
Argumentai	txHash – *Bitcoin* finansinės operacijos id. Pvz.: fd8f05c426752b9c4fd642c58311ebffafccbbca2c2f51c183240f7b19a9f654
Tipas	GET
Aprašymas	Ši programinė sąsaja gauna finansinės operacijos identifikatorių, pagal tai iš *blockchain.info* programavimo sąsajos paimami duomenys, jie normalizuojami, užkraunamas ištreniruotas modelis. Finansinė operacija klasifikuojama, grąžinami neapdorotos finansinės operacijos duomenys, klasifikavimo rezultatas.
Galimi atsakymai	200 – finansinė operacija sėkmingai rasta ir klasifikuota 404 – finansinės operacijos id nebuvo rastas *Bitcoin* tinkle 500 – klaida klasifikuojant finansinę operaciją

Tipinis atsakas	{
	"txHash": "fd8f05c426752b9c4fd642c58311ebffafccbbca2c2f51c183240f7b19a9f654",
	"isLegal": false,
	"rawTx": {
	Neapdoroti finansinės operacijos duomenys...
	}
	}

5 lentelė. Piniginės finansinių operacijų klasifikavimo programinė sąsaja

Pavadinimas	Klasifikuoti *Bitcoin* piniginės finansines operacijas pagal adresą
Kelias	http://127.0.0.1:8000/wallet/?walletAddr={walletAddr}
Argumentai	walletAddr – *Bitcoin* piniginės adresas. Pvz.: bc1q9p3te2xaffazeak80ljrvja9qpr4hluyg2cfak
Tipas	GET
Aprašymas	Ši programinė sąsaja gauna *Bitcoin* piniginės adresą, pagal tai gauna naujausias (iki 100) finansinių operacijų. Toliau kiekviena finansinė operacijas klasifikuojama į legalias ir nelegalias. Grąžinamas masyvas finansinių operacijų, kurių kiekviena turi atributą *isLegal*, kuris nurodo modelio klasifikavimo rezultatą.
Galimi atsakymai	200 – Piniginė sėkmingai rasta ir jos finansinės operacijos suklasifikuotos 404 – piniginės adreso nepavyko rasti *Bitcoin* tinkle 500 – klaida klasifikuojant piniginės finansines operacijas

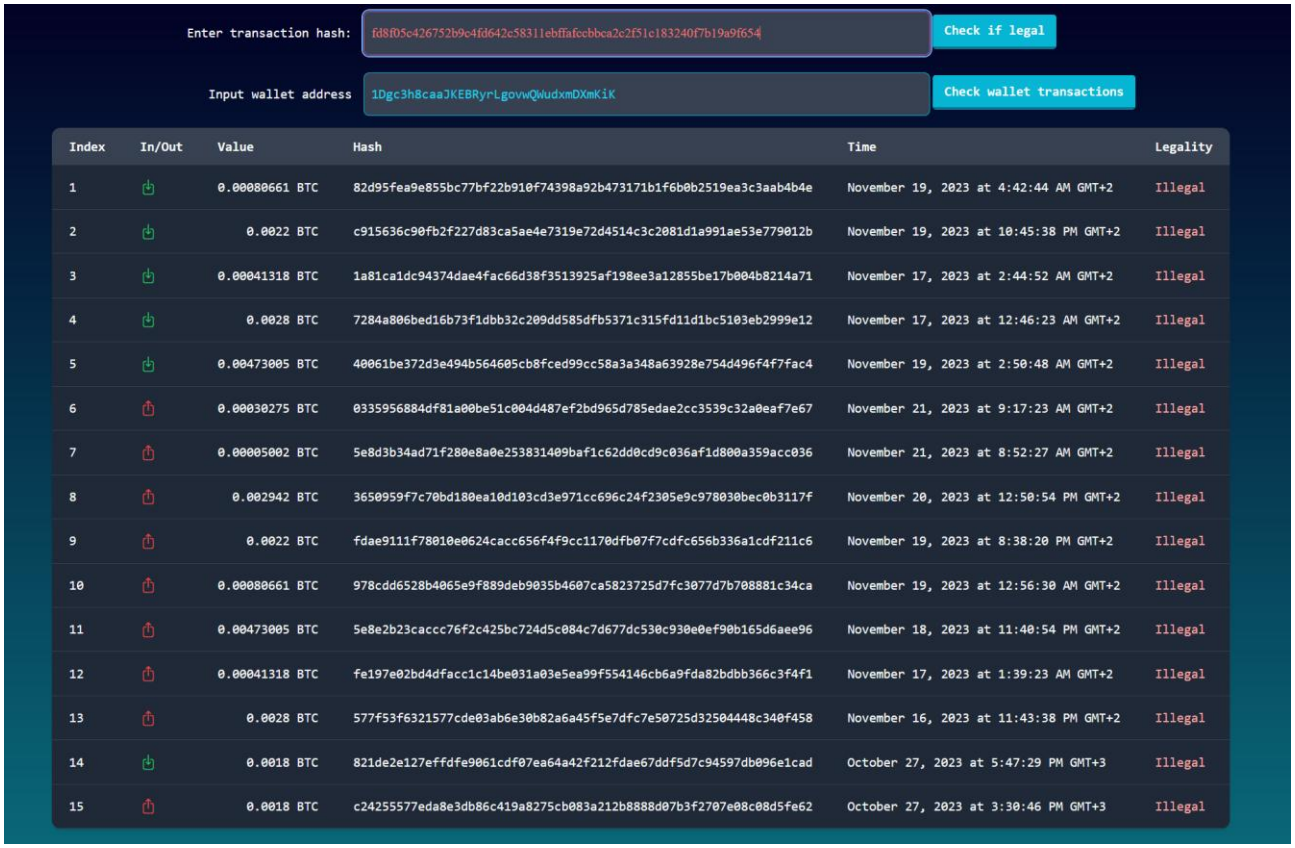
Tipinis atsakas	[
	{
	"isLegal": false,
	"rawTx": {
	"hash": "fd8f05c426752b9c4fd642c58311ebffafccbbca2c2f51c183240f7b19a9f654",
	Kiti finansinės operacijos atributai ...

```
                    }
        },
        {
            "isLegal": true,
            "rawTx": {
                "hash": "82d95fea9e855bc77bf22b910f74398a92b473171b1f6b0b2519ea3c3aab4b4e",
                Kiti finansinės operacijos atributai ...
                    }
        },
]
```


4 lentelėje ir 5 lentelėje aprašyti, programavimo sąsajos taškai, į kuriuos galima kreiptis.

3.7. Finansinių operacijų analizavimo įrankis

Finansinių operacijų analizavimo įrankio naudotojo sąsaja sukurta naudojantis *Node.js*, *React* ir *typescript* technologijas (23 pav.).



Index	In/Out	Value	Hash	Time	Legality
1	↓	0.00080661 BTC	82d95fea9e855bc77bf22b910f74398a92b473171b1f6b0b2519ea3c3aab4b4e	November 19, 2023 at 4:42:44 AM GMT+2	Illegal
2	↓	0.0022 BTC	c915636c90fb2f227d83ca5ae4e7319e72d4514c3c2081d1a991ae53e779012b	November 19, 2023 at 10:45:38 PM GMT+2	Illegal
3	↓	0.00041318 BTC	1a81ca1dc94374dae4fac66d38f3513925af198ee3a12855be17b004b8214a71	November 17, 2023 at 2:44:52 AM GMT+2	Illegal
4	↓	0.0028 BTC	7284a806bed16b73f1dbb32c209dd585dfb5371c315fd11d1bc5103eb2999e12	November 17, 2023 at 12:46:23 AM GMT+2	Illegal
5	↓	0.00473005 BTC	40061be372d3e494b564605cb8fced99cc58a3a348a63928e754d496f4f7fac4	November 19, 2023 at 2:50:48 AM GMT+2	Illegal
6	↑	0.00030275 BTC	0335956884df81a00be51c004d487ef2bd965d785edae2cc3539c32a0eaf7e67	November 21, 2023 at 9:17:23 AM GMT+2	Illegal
7	↑	0.00005002 BTC	5e8d3b34ad71f280e8a0e253831409baf1c62dd0cd9c036af1d800a359acc036	November 21, 2023 at 8:52:27 AM GMT+2	Illegal
8	↑	0.002942 BTC	3650959f7c70bd180ea10d103cd3e971cc696c24f2305e9c978030bec0b3117f	November 20, 2023 at 12:50:54 PM GMT+2	Illegal
9	↑	0.0022 BTC	fdae9111f78010e0624cacc656f4f9cc1170dfb07f7cdfc656b336a1cdf211c6	November 19, 2023 at 8:38:20 PM GMT+2	Illegal
10	↑	0.00080661 BTC	978cdd6528b4065e9f889deb9035b4607ca5823725d7fc3077d7b708881c34ca	November 19, 2023 at 12:56:30 AM GMT+2	Illegal
11	↑	0.00473005 BTC	5e8e2b23caccc76f2c425bc724d5c084c7d677dc530c930e0ef90b165d6aee96	November 18, 2023 at 11:40:54 PM GMT+2	Illegal
12	↑	0.00041318 BTC	fe197e02bd4dfacc1c14be031a03e5ea99f554146cb6a9fda82bdbb366c3f4f1	November 17, 2023 at 1:39:23 AM GMT+2	Illegal
13	↑	0.0028 BTC	577f53f6321577cde03ab6e30b82a6a45f5e7dfc7e50725d32504448c340f458	November 16, 2023 at 11:43:38 PM GMT+2	Illegal
14	↓	0.0018 BTC	821de2e127effdfe9061cdf07ea64a42f212fdae67ddf5d7c94597db096e1cad	October 27, 2023 at 5:47:29 PM GMT+3	Illegal
15	↑	0.0018 BTC	c24255577eda8e3db86c419a8275cb083a212b8888d07b3f2707e08c08d5fe62	October 27, 2023 at 3:30:46 PM GMT+3	Illegal

23 pav. Naudotojo sąsaja atvaizduojanti piniginės finansines operacijas

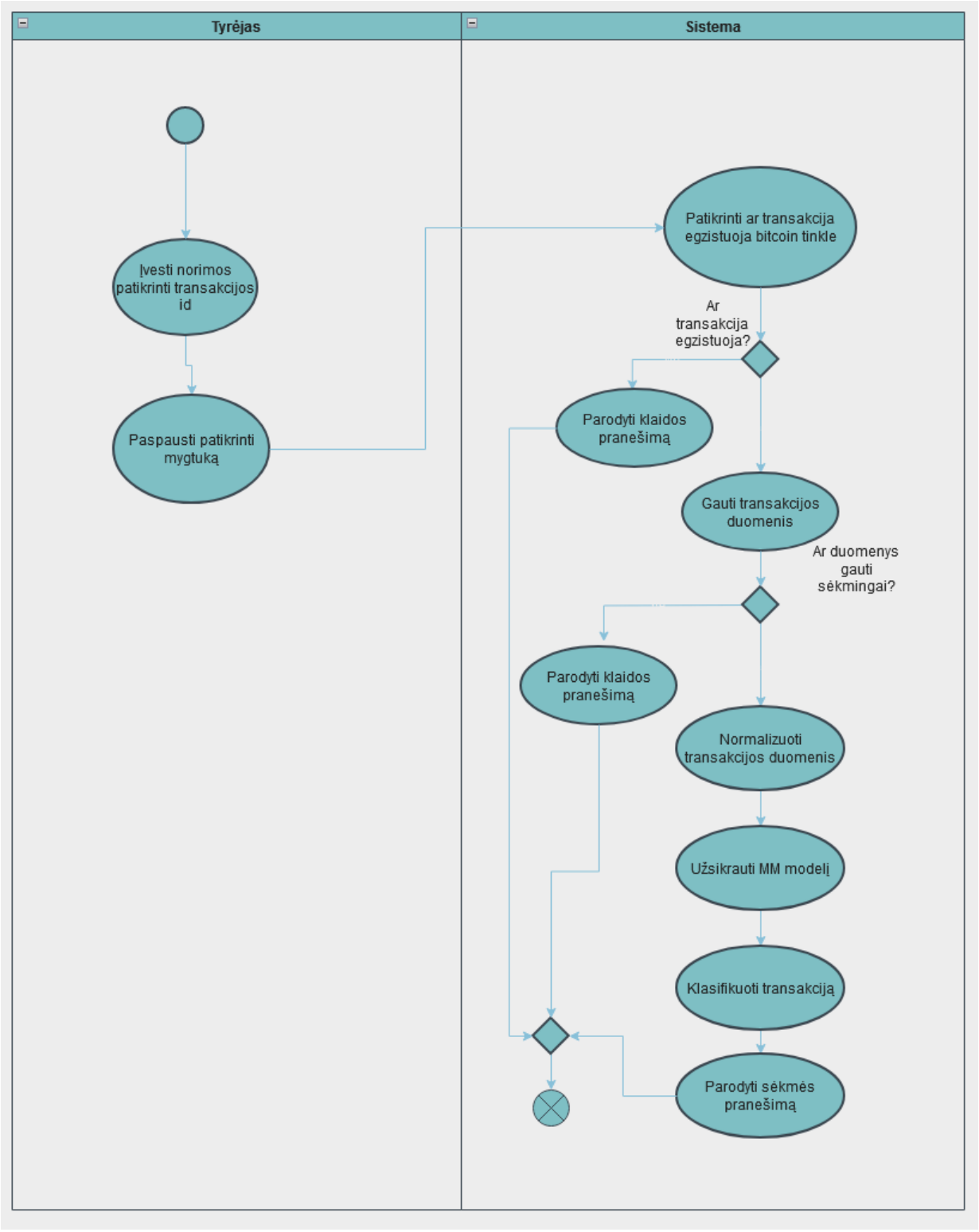
Kiekviena iš finansinių operacijų gali būti analizuojama individualiai (24 pav.).

24 pav. Naudotojo sąsaja finansinės operacijos analizavimui

Įrankis turi galimybę analizuoti konkrečią finansinę operaciją. Šiuo konkrečiu atveju (24 pav.), ekrane matomi šie elementai:

- Modelio atliktos finansinės operacijos patikros rezultatas bei svarbiausi finansinės operacijos duomenys – atlikimo data, įėjimų kiekis, išeities kiekis, mokestis, bloko identifikatorius.
- Sistema pasinaudodama *SHAP* klasifikatorių analizės biblioteka, ekrane atvaizduoja kaip buvo atliktas sprendimas finansinę operaciją klasifikuoti būtent šitaip. Paveiksliuką reiktų interpretuoti kaip virvės traukimą – vieni kintamieji traukia modelio pasirinkimą į legalią pusę, kiti į nelegalią. Šiuo atveju laimi legali pusė (raudona spalva).

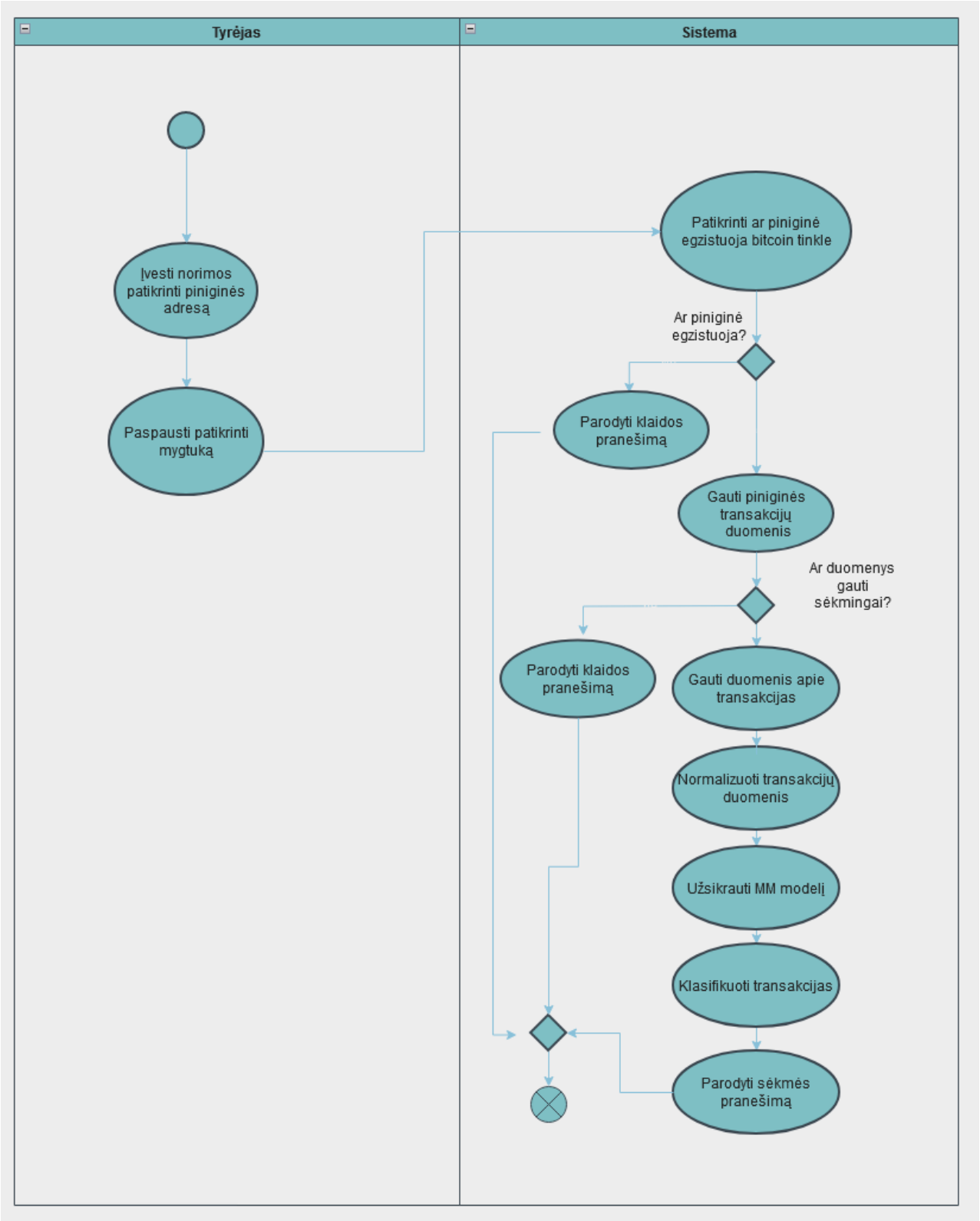
Tyrėjui įvedus norimą patikrinti finansinės operacijos identifikatorių ir paspaudus mygtuką „*Check if legal*“ sistema atlieka sekančius veiksmus (25 pav. , 6 lentelė).



25 pav. Panaudos atvejo „Klasifikuoti finansinę operaciją“ sekų diagrama

6 lentelė. Panaudos atvejo „Klasifikuoti finansinę operaciją“ aprašymas

PA. Klasifikuoti finansinę operaciją		
Tikslas. Naudotojui nurodžius finansinės operacijos ID, klasifikuoti ją pagal jos legalumą		
Aprašymas. Sistemos naudotojas į teksto lauką įveda finansinės operacijos identifikatorių, sistema patikrina ar finansinė operacija yra teisinga, jeigu taip gaunami finansinės operacijos duomenys, jie normalizuojami, užkraunamas pasirinktas modelis, finansinė operacija klasifikuojama, parodomas rezultatas.		
Prieš sąlyga		-
Aktoriai		Sistemos naudotojas
Susiję panaudojimo atvejai	**Išplečiantys PA**	-
	Apimami PA	-
	Specializuojami PA	-
Po sąlyga		Naudotojui parodoma ar finansinė operacija legali ar ne



26 pav. Panaudos atvejo „Klasifikuoti piniginės finansines operacijas“ sekų diagrama

26 pav. ir 7 lentelė. atvaizduoti žingsniai, kuriuos atlieka sistema tyrėjui paprašius klasifikuoti *bitcoin* piniginės finansines operacijas.

7 lentelė. Panaudos atvejo „Klasifikuoti piniginės finansines operacijas“ aprašymas

PA. Klasifikuoti piniginės finansines operacijas		
Tikslas. Klasifikuoti naudotojo nurodytos piniginės finansines opracijas į legalias ir nelegalias		
Aprašymas. Sistemos naudotojas įveda piniginės adresą, sistema patikrina ar nurodytas adresas egzistuoja, tuomet gaunamos visos piniginės finansinės operacijos, jų duomenys normalizuojami, kiekviena finansinė operacija klasifikuojama, ekrane parodomas rezultatas lentele.		
Prieš sąlyga. -		-
Aktoriai		Sistemos naudotojas
Susiję panaudojimo atvejai	**Išplečiantys PA**	-
	Apimami PA	-
	Specializuojami PA	-
Po sąlyga		Naudotojui parodomos nurodytos piniginės finansinės operacijos lentele, vienas iš stulpelių nurodo operacijų legalumą

3.8. Įrankio pritaikymas realioms finansinėms operacijoms klasifikuoti

ChainAbuse – tarptautinė platforma, skirta paskelbti piniginių, galimai dalyvavusių nelegaliose veikose adresus. Ši platforma pateikia išsamų ataskaitų apie nelegalias veiklas rinkinį, kuris apima sukčiavimus, šantažą, išpirkos reikalavimus ir kitas nelegalias veiklas. Šios platformos pagalba buvo pasirinkta ištirti 10 skirtingų tipų piniginių, kurios galimai buvo įtrauktos į nelegalias veiklas.

8 lentelė. Piniginių įtrauktų į nelegalias veiklas tyrimas

	Nelegalios veiklos tipas	Piniginės adresas	Prognozuojamas nelegalių finansinių operacijų skaičius piniginėje	Prognozuojamas legalių finansinių operacijų skaičius piniginėje	Procentas nelegalių finansinių operacijų
1	Sukčiavimas (angl. *phishing*)	1Dgc3h8caaJKEBRyrLgovwQWudxmDXmKiK	9	6	60%
2	Išpirkos reikalaujanti programinė įranga	bc1qx28mz579uq0h7s4kf9mu5qu8u53pr4kfqmkl7f	6	0	100%
3	Apsimetinėjimas kitu asmeniu	1CefBdUBFFTfY9bJ831fYhR2zPRAdi66mg	2	2	50%
4	Šantažas	15PjLxvFvVuUASkWLTReBDf1SAnGboiE3Q	1	0	100%
5	Netikri prekių grąžinimai	bc1q0av4lzqldysdjv2tdyd02es79yhs5hdke5x0dn	18	0	100%
6	Romantika	1C9roKKGjgb2WyaYTMnQAStbhYoH4TVHwu	26	1	96%
7	Sukčiavimas	1Dgc3h8caaJKEBRyrLgovwQWudxmDXmKiK	9	6	60%
8	Seksualinės paslaugos	bc1qrwjt8xhs7z02fduywjym33eteas5kqg8dncnwt	4	0	100%
9	Kitokie įsilaužimai	bc1qn3uctqzgy5tnw5g4kf556a5l5j4fuj8cys36f9	6	0	100%
10	Išpirkos reikalaujanti programinė įranga	3PXh2r3XP9zYcceAJ8SweKqfbkuxQNmUEu	97	3	97%

Ištyrus 10 piniginių susijusių su įvairiais skaitmeniniais nusikaltimais *bitcoin* blokų grandinėse, kiekvienoje bent dalis finansinių operacijų buvo klasifikuotos kaip nelegalios (8 lentelė.). Galima teigti – įrankis geba atpažinti pinigines, kurios dalyvavo nelegaliose veiklose. Šis testas parodo ne tik teorines modelio galimybes, bet ir praktinį pritaikymą.

3.9. Apibendrinimas

Sukurtas prototipas yra grįstas *Elliptic* duomenų rinkiniu bei yra praturtintas galimybe klasifikuoti nežinomas duomenų rinkinyje nematytas finansines operacijas. Prototipas naudoja mašininio mokymosi modelį *XGBoost,* klasifikuoja Bitcoin finansines operacijas. Programinis kodas patalpintas į *github* programinio kodo saugyklą[20].

Šis prototipas yra žingsnis griežtesnės kriptovaliutų kontrolės link, kuris gali padėti *bitcoin* tinklų tyrėjams analizuoti finansines operacijas ir jų legalumą. Jis nėra tobulas, tačiau turi potencialą būti naudingu įrankiu *bitcoin* tyrimams.

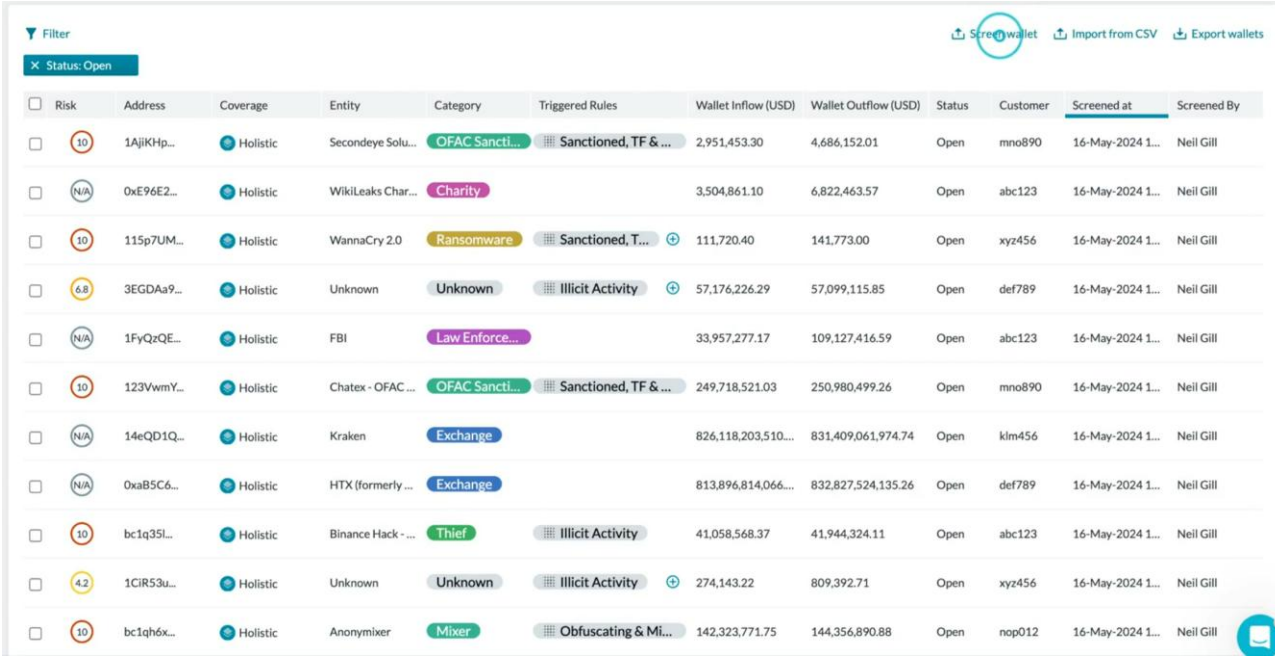
4. Eksperimentas

4.1. Kokybinis vertinimas

Rinkoje šiuo metu egzistuoja keletas sprendimų kriptovaliutų blokų grandinių analizei atlikti. Šie sprendimai įprastai yra skirti teisėsaugai, pinigų plovimo prevencijos skyriams, mokesčių agentūroms, bei privatiems sektoriams.

4.1.1. Elliptic Lens

Įmonės pateikusios šiame darbe naudotą *bitcoin* finansinių operacijų duomenų rinkinį sukurtas galingas įrankis (27 pav.). Didžiausias sprendimo privalumas, gebėjimas analizuoti pinigų srautus tarp skirtingų blokų grandinių (šiuo metu palaikomos 47 kriptovaliutos). Tai pasiekiama sukuriant vieną didžiulį finansinį tinklą, kuris sudarytas iš milijonų duomenų taškų, kurie atspindi visą kriptovaliutų finansinę sistemą. Šis pranašumas leidžia *Elliptic Lens* naudotojams pastebėti rizikas kurios nebūtų matomos analizuojant tik vieną kriptovaliutų tinklą (pvz. *Bitcoin*)[36].



27 pav. *Elliptic Lens*[36]

Šis įrankis taip pat yra didesnio paketo – *Elliptic Nexus* daslis, kuris šiuo metu yra privačių įmonių rinkos lyderis – jį naudoja didžiausios kriptovaliutų keityklos – *Binance* ir *Coinbase*, taip pat kitos finansinės įmonės – *Revolut*, *Paysafe* pinigų plovimo prevencijai vykdyti.

4.1.2. Chainalysis

Chainalysis siūlomi įrankiai taip pat yra vieni iš rinkos lyderių, juos naudoja virš 1400 klientų, tarp jų – *Barclays*, *Microsoft*, *Gemini*. Jis gerai žinomas teisėsaugos srityje, dažnai naudojami valstybinėse institucijose.

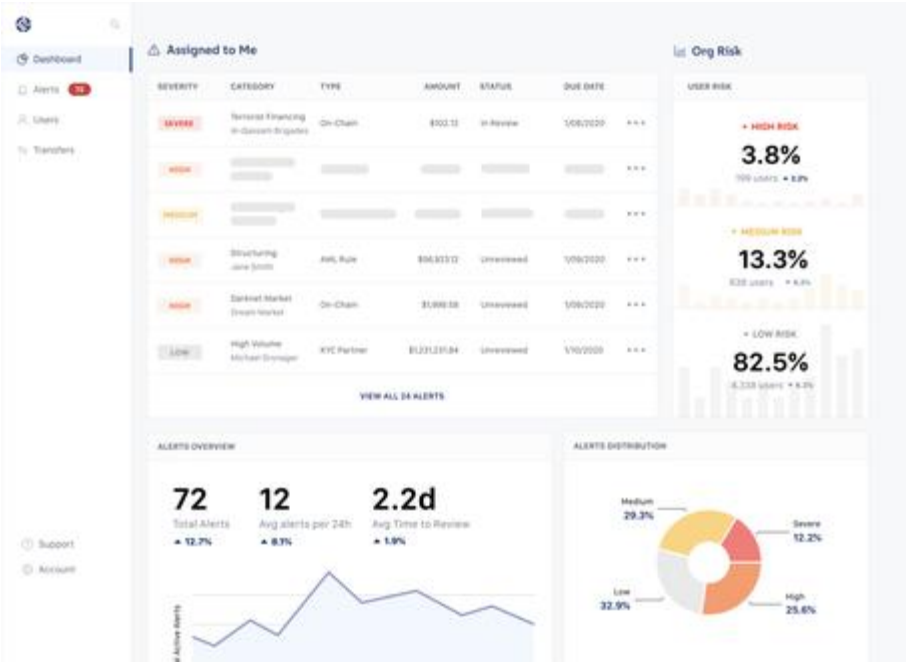
Chainalysis programinė įranga suteikia tokias galimybes:

- Neteisėtos veiklos nustatymas - padeda teisėsaugos institucijoms, vyriausybinėms agentūroms ir finansų įstaigoms nustatyti ir ištirti neteisėtą veiklą, susijusią su kriptovaliutomis, tokią kaip pinigų plovimas, terorizmo finansavimas, atsiskaitymai juodojoje rinkoje ir sukčiavimas.

- Finansinių operacijų stebėjimas – įmonė suteikia įrankius bei duomenis, kurie leidžia aktyviai stebėti finansines operacijas realiu laiku, nustatyti įtartinus lėšų srautus, gauti pranešimus susijusius su nelegaliomis veikomis.

- Tyrimai ir analizė – be programinės įrangos, *chainalysis* teikia paslaugą atlikti išsamius kriptovaliutų tinklo tyrimus, sukurti ataskaitas, pasidalyti ekspertinėmis žiniomis su visuomene.

Vienas pagrindinių įmonės sprendimų – *X-sight* (28 pav.).



28 pav. *Chainalysis X-sight* programinė įranga[35]

Vienas didesnių šio produkto privalumų – integracija su jau egzistuojančiu, plačiai naudojamu pinigų plovimo prevencijos produktu „*NICE Actimize*“

4.1.3. Skirtumai tarp esamų sprendimų ir sukurto prototipo

Rinkoje egzistuojantys sprendimai yra orientuoti į asmenį, ir stengiasi atlikti asmens piniginių srautų analizę ne viename blokų grandinių tinkle o sudaryti tarptinklinį kriptoturto grafą, tuo tarpu sukurtas sprendimas orientuotas tik į *bitcoin* finansinių operacijų analizę. Sukurtas sprendimas kitaip nei rinkoje egzistuojantys sprendimai turi galimybę paaiškinti savo sprendimus naudojant *SHAP* analizę.

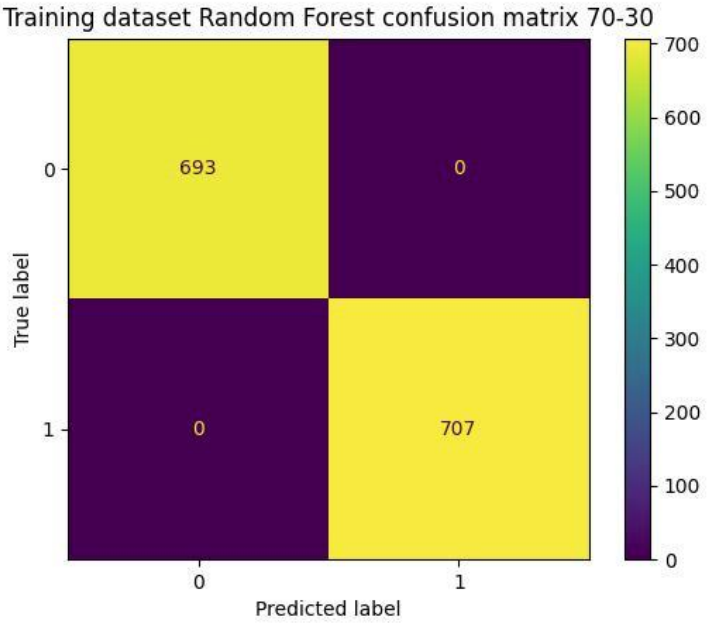
Lyginant sukurtą kriptovaliutų finansinių operacijų analizės įrankį su rinkoje esančiais komerciniais sprendimais, susiduriama su riboto viešo prieinamumo iššūkiu dėl šių įrankių privatumo. Analizuotos komercinės platformos skirtos verslo klientams ir neturi viešai prieinamų demonstracinių versijų,

skirtų išsibandyti individualiems tyrėjams ar akademiniams tikslams, todėl atlikti gilesnę analizę yra neįmanoma.

4.2. Kiekybinis vertinimas

4.2.1. Persimokymo vertinimas

Persimokymas – reiškinys, kuomet mašininio mokymosi algoritmas per daug prisitaiko prie treniravimosi duomenų. Tai reiškia modelis nėra bendrai tinkamas naujiems jam nematytiems duomenims. Tam, kad patikrinti ar modelis nepersimokė, tikrinama kaip modelis klasifikuoja duomenis kurie buvo naudojami jo apmokymui (29 pav.).



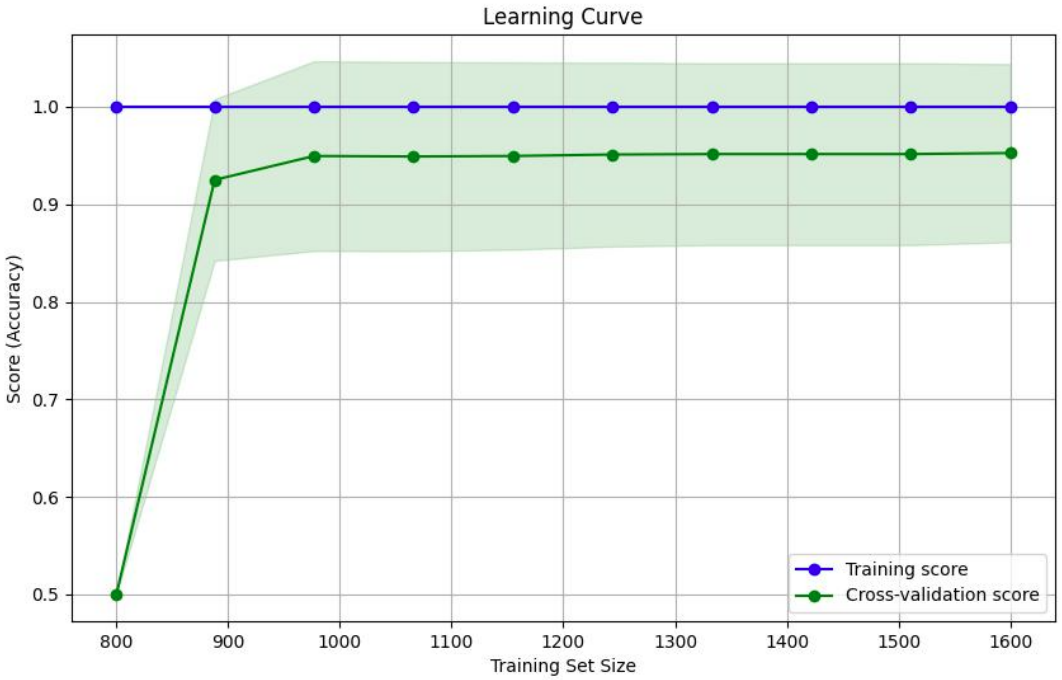
29 pav. Treniravimosi duomenų klasifikavimas naudojant atsitiktinį mišką

Matoma, kad modelis nei karto nesuklydo spėdamas duomenis. Modelio tikslumas skaičiuojamas naudojant šią formulę:

$$Tikslumas = \frac{(TP + TN)}{(TP + TN + FP + FN)} = \frac{Teisingai\ klasifikuotų\ stebinių\ skaičius}{Visų\ stebinių\ skaičius}$$

Konkrečiu atveju (29 pav.) modelio tikslumas su duomenimis kuriais modelis apsimokė - 100%, tai reiškia modelis persimokė.

Išbandoma didinti stebinių skaičių iki 2000 (30 pav.).



30 pav. Tikslumo priklausomybė nuo stebinių skaičiaus

Matoma, kad net ir didinant duomenų kiekį, modelio persimokymui tai įtakos neturi, viršutinė mėlynoji tiesė visada siekia 1. Siekiant sumažinti modelio persimokymą, deriname modelių hiperparametrus.

4.2.2. Atsitiktinio miško hiperparametrų derinimas

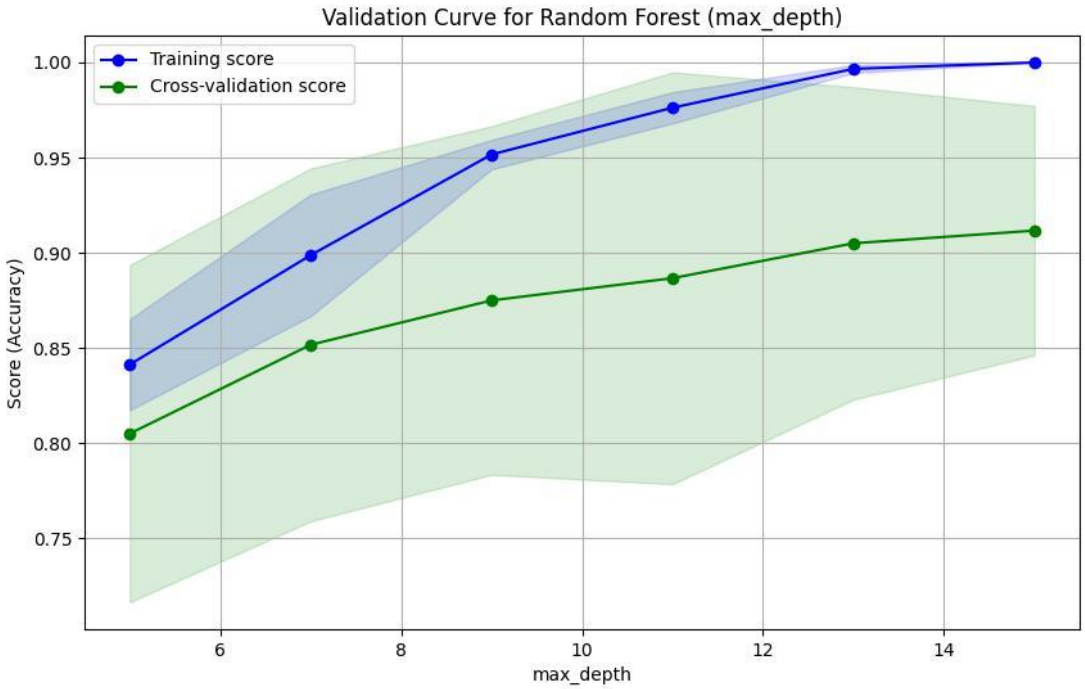
Hiperparametrų derinimas naudingas ne tik norint išvengti persimokymo, šis procesas gali pagerinti modelių rezultatus, optimizuoti modelio prognozavimo laiką, sumažinti modelio resursų poreikį.

Pagrindiniai parametrai, kurios galima derinti atsitiktinio miško ir jo atmainų modeliuose:

- Maksimalus medžio gylis (angl. *max_depth*)
- Maksimalus požymių skaičius (angl. *max_features*)
- Minimalus stebinių skaičius reikalingas mazgo padalijimui (angl. *min_samples_split*)
- Medžių skaičius (angl. *n_estimators*)

Parametrų tinkamumas bus atrenkamas naudojant validavimo kreives. Jos padeda vizualiai suprasti, kaip modelio veikimas keičiasi, keičiant tam tikrus modelio parametrus.

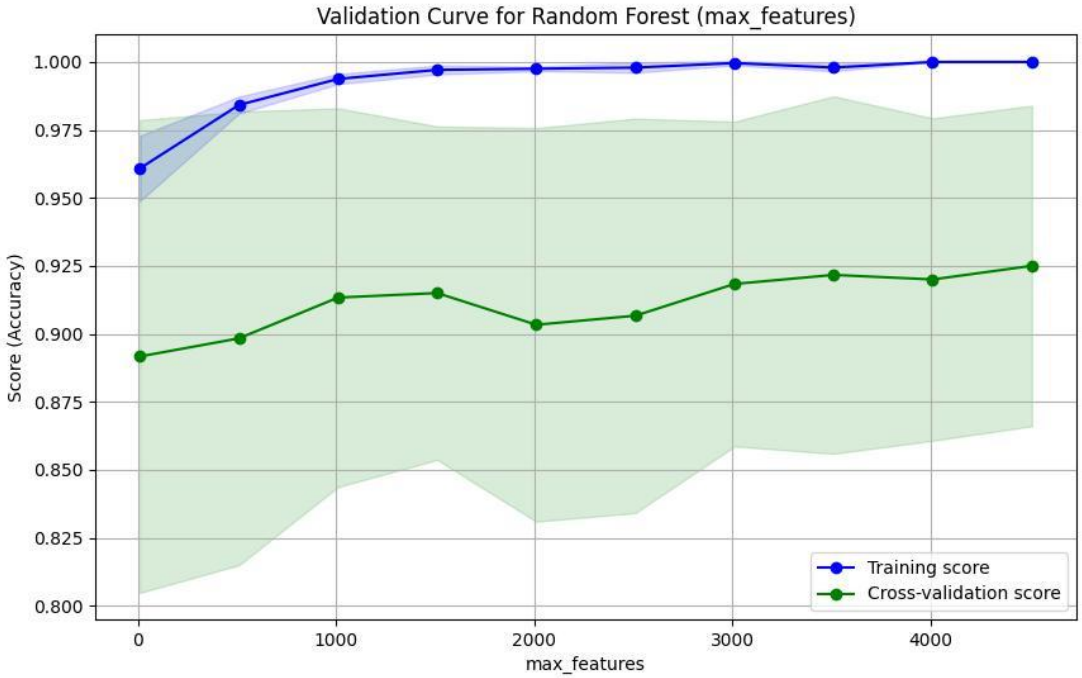
Žalioji linija grafikuose žymi kryžminio validavimo rezultatą, kuris vizualiai apibendrina kaip tiksliai modelis klasifikuoja naujus, nematytus duomenis. Mėlynoji linija nurodo kaip tiksliai modelis klasifikuoja duomenis, kurie buvo naudojami apmokymui.



31 pav. Maksimalaus medžio gylio validavimo kreivė

Didėjant medžio gyliui modelis sudėtingėja ir teisingiau klasifikuoja, visgi, prie maksimalaus medžio gylio 13, modelio tikslumas prognozuojant treniravimo imtį priartėja prie 1, tai reiškia modelis pradeda persimokyti (31 pav.). Šiuo atveju geriausia parametro vertė ~12 – taip modelis nepersimoko.

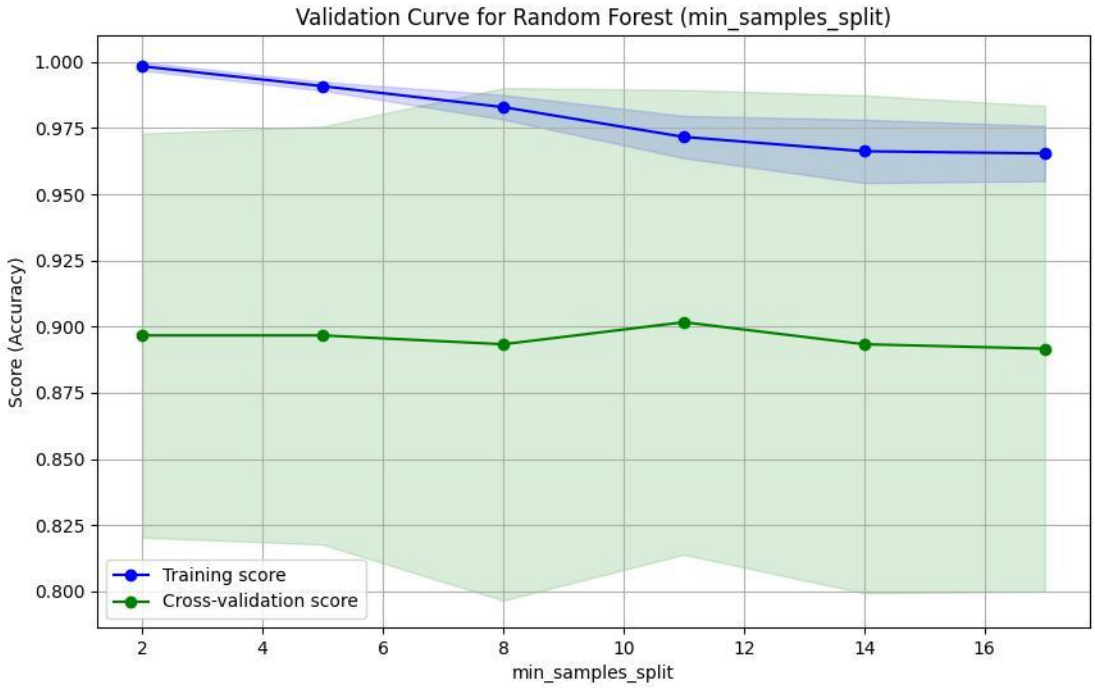
Toliau atliekamas hiperparametro limituojančio naudojamų požymių skaičių derinimas (32 pav.).



32 pav. Atsitiktinai parenkamų savybių skaičiaus validavimo kreivė

Naudojant daugiau nei 1500 požymių sprendimo medžiai pradeda persimokyti, šiuo atveju geriausias pasirinkimas yra intervale [1000; 1500]. Visgi reikėtų įvertinti, kad naudojant žemesnį parametrą modelis yra paprastesnis ir spėjimus turėtų atlikti greičiau, naudoti mažiau kompiuterio resursų.

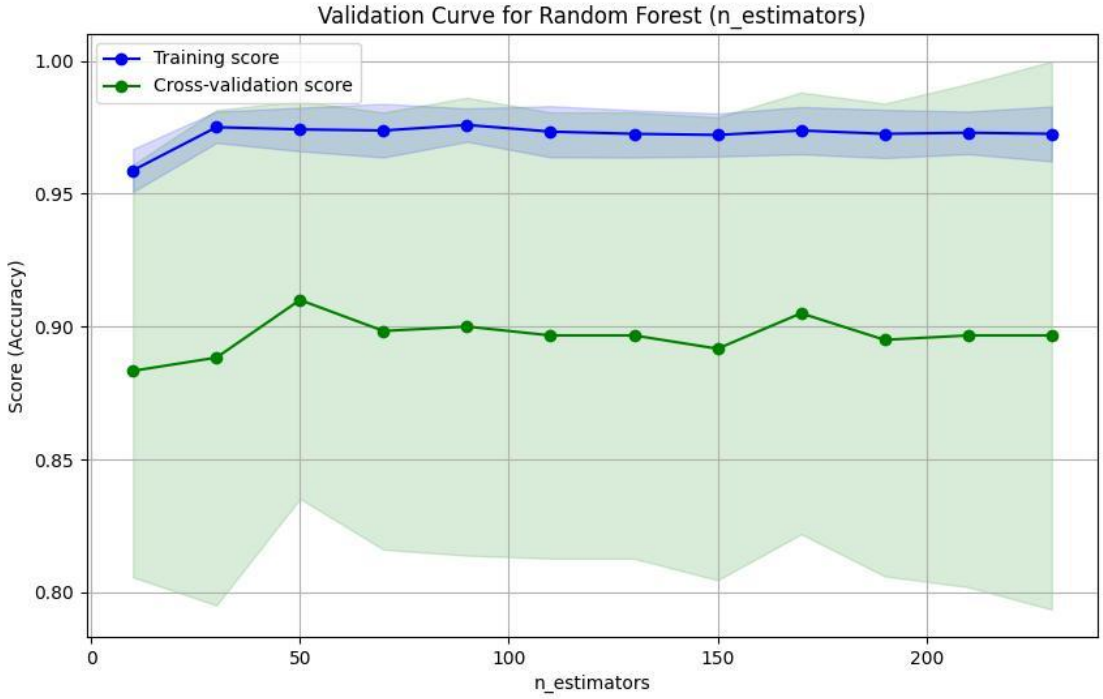
Toliau atliekamas hiperparametro limituojančio stebinių reikalingų mazgo padalijimui skaičiaus derinimas (33 pav.).



33 pav. Minimalaus stebinių skaičiaus reikalingų mazgo padalijimui validavimo kreivė

Leidžiant modeliui kurti mazgus su 2 stebiniais, jis stipriai persimoko, didinant šį skaičių persimokymas (mėlyma kreivė) mažėja. Aukščiausias kryžminio validavimo rezultatas pasiekiamas maždaug ties 10-12. Šiame intervale modelis turi geriausią pusiausvyrą tarp prisitaikymo prie duomenų ir gebėjimo generalizuoti.

Toliau atliekamas hiperparametro nurodančio medžių skaičių derinimas (34 pav.).



34 pav. Atsitiktinio miško medžių skaičius

Kryžminio validavimo reikšmė stabiliai aukšta, remiantis tuo optimali parametro reikšmė galėtų būti intervale [50; 200], visgi mažesnis medžių skaičius gali būti nepakankamas stabilumui, todėl šiuo atveju parenkama parametro vertė – 100.

Geriausi atsitiktinio miško parametrai:

- Maksimalus medžio gylis - 12
- Maksimalus požymių skaičius - 1000
- Minimalus stebinių skaičius reikalingas mazgo padalijimui - 10
- Medžių skaičius – 100

4.2.3. *ADA Boost* ir *XG Boost* modelių hiperparametrai

Modelio hiperparametrams suderinti naudojama tinklelio geriausių parametrų paieška *GridSearchCV*, kuri yra dalis *python* bibliotekos *sklearn*. Hiperparametrų paieška veikia tokiu principu:

- Sukuriamas tinklelis su reikšmėmis, kurias norima keisti.
- Nustatomi tinklelio paieškos parametrai, kryžminės validacijos strategija.
- Paieška iteruoja per visas įmanomas pateikto tinklelio parametrų kombinacijas, apskaičiuoja vidutinį kryžminės validacijos metu gautą tikslumą.

- Nustatomi geriausi hiperparametrai.

Hiperparametrų paieškai bazinis klasifikatorius bus naudojamas atsitiktinis medis su geriausiais atsitiktinio miško medžio parametrais gautais nagrinėjant atsitiktinio miško hiperparametrus, tuo tarpu paieškos tinklelis atrodo taip (9 lentelė):

9 lentelė. *ADABoost* bei *XGBoost* modelių hiperparametrų tinklelio paieškos parametrai

Hiperparametro pavadinimas	Tinklinės paieškos reikšmės
Medžių skaičius (angl. *n_estimators*)	50, 100, 200
Mokymosi greitis (angl. *learning_rate*)	0.01, 0.1, 0.5, 1

Atlikus paiešką geriausi hiperparametrai *ADA Boost* modeliui:

- Medžių skaičius – 100
- Mokymosi greitis – 0.01

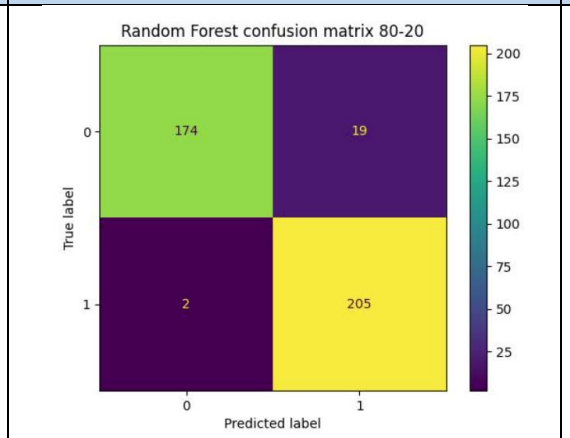
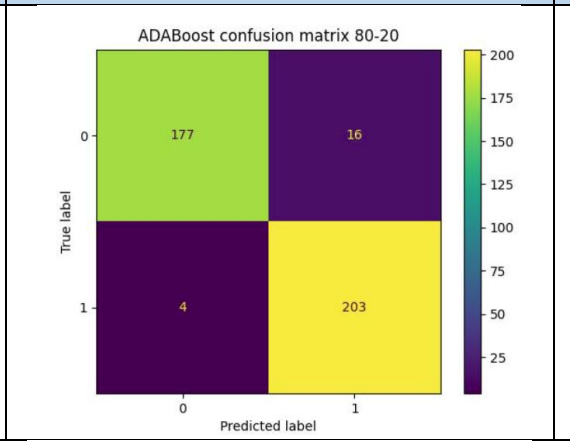
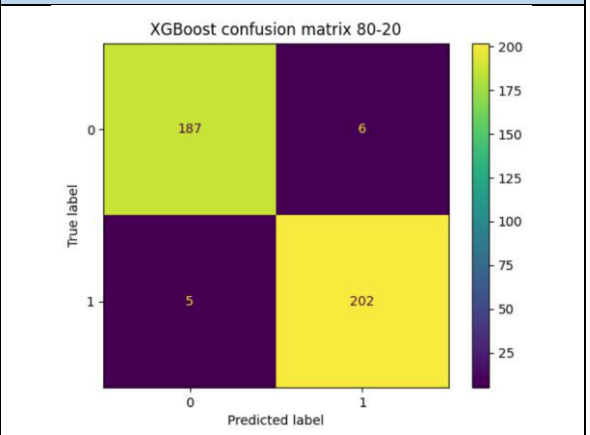
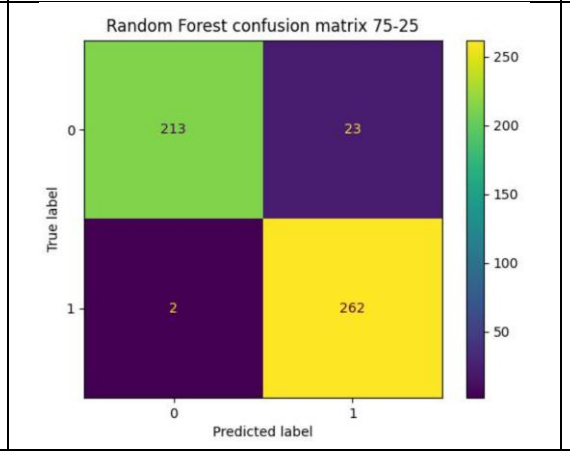
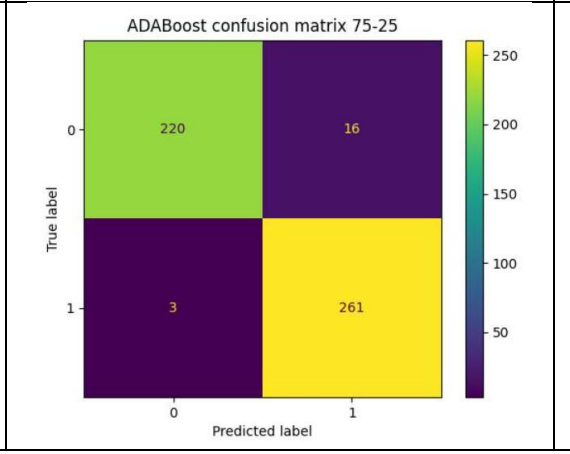
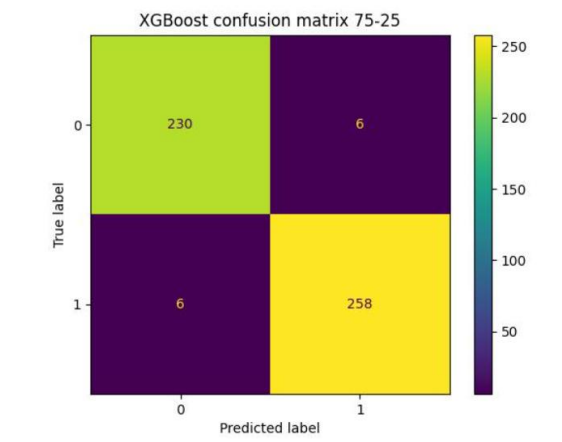
Geriausi hiperparametrai *XGBoost* modeliui:

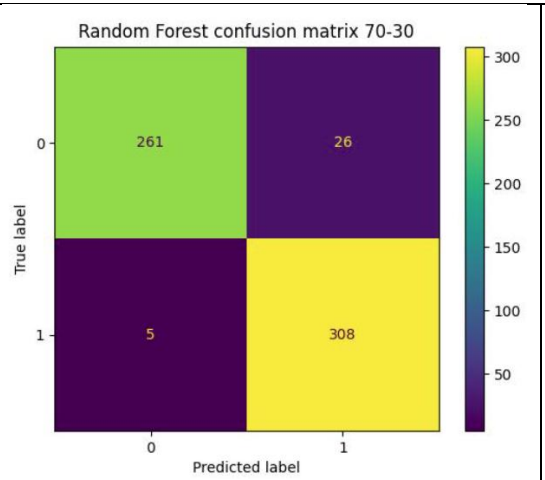
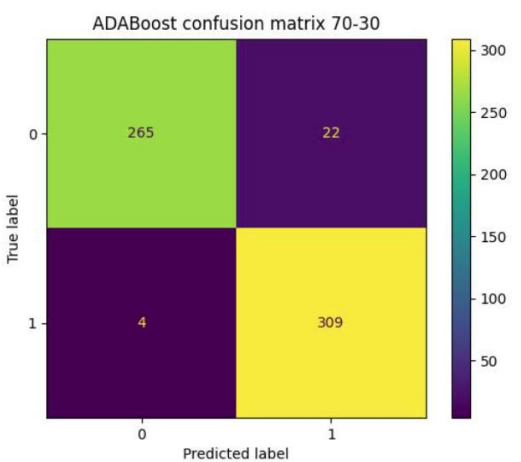
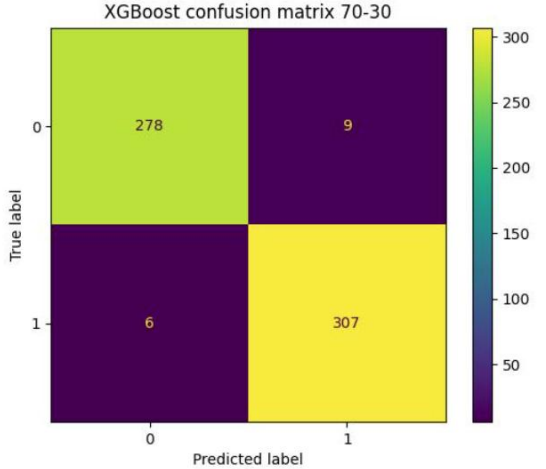
- Medžių skaičius – 150
- Mokymosi greitis – 0.01

4.2.4. Skirtingi treniravimo ir testavimo imčių santykiai

Norint sukurti patikimą mašininio mokymosi modelį, reikia išbandyti skirtingus treniravimo bei testavimo imčių santykius, tai padeda atrasti modelį kuris turi didžiausią tikslumą, nepersimoko (10 lentelė.).

10 lentelė. Mašininio mokymosi modelių rezultatų palyginimas – klaidų matricos (testavimo imtis)

Treniravimo / testavimo imčių santykis	**Random Forest**	**ADA_Boost**	**XG_Boost**
80/20			
75/25			

70/30			

11 lentelė. Mašininio mokymosi modelių rezultatų palyginimas – bendras tikslumas (testavimo imtis)

Treniravimo / testavimo imčių santykis	**Random Forest**	**ADA Boost**	**XG Boost**
80/20	0.947	0.950	0.972
75/25	0.950	0.962	0.976
70/30	0.948	0.956	0.975

Galima matyti, kad visais trimis nagrinėjamais duomenų dalijimo santykiais geriausią rezultatą parodė *XGBoost* algoritmas, antroje vietoje buvo *ADABoost* (11 lentelė.). Naudojant gradientinio stiprinimo modelį bei skeliant duomenis į treniravimo ir testavimo imtis santykiu 75/25, buvo gautas net 0.976 tikslumas. 10 lentelė. grafikuose galima matyti, kad visi modeliai antro tipo klaidas (klaidingai teigiami) daro dažniau, šiuo atveju tai reiškia, kad modeliai dažniau nelegalias finansines operacijas klasifikuoja kaip legalias, nei legalias kaip nelegalias.

Dirbant su sukčiavimo aptikimu svarbu aptikti kuo daugiau sukčiavimo atvejų (aukštas jautrumas), ir sumažinti klaidingus signalus (aukštas tikslumas). Šiuos parametrus vertiname skaičiuodami modelio F1 balą:

$$F1 = 2 \times \frac{Tikslumas \times Jautrumas}{Tikslumas + Jautrumas} = \frac{2TP}{2TP + FP + FN}$$

$$F1 = \frac{2 * 258}{2 * 258 + 6 + 6} \approx 0.9773$$

XGBoost modelio, treniruoto su testavimo / treniravimo imties santykiu 25 / 75, F1 balas yra apie 0.9773, tai atskleidžia, kad modelis pasiekė labai gerą pusiausvyrą tarp tikslumo ir jautrumo klasifikuojant duomenis.

Toliau tikrinama ar modeliai nėra persimokę, tai atliekama klasifikuojant naudotą treniravimo imtį, jeigu modeliai per daug prisitaikė prie gautų duomenų klasifikavimo tikslumas sieks 100%.

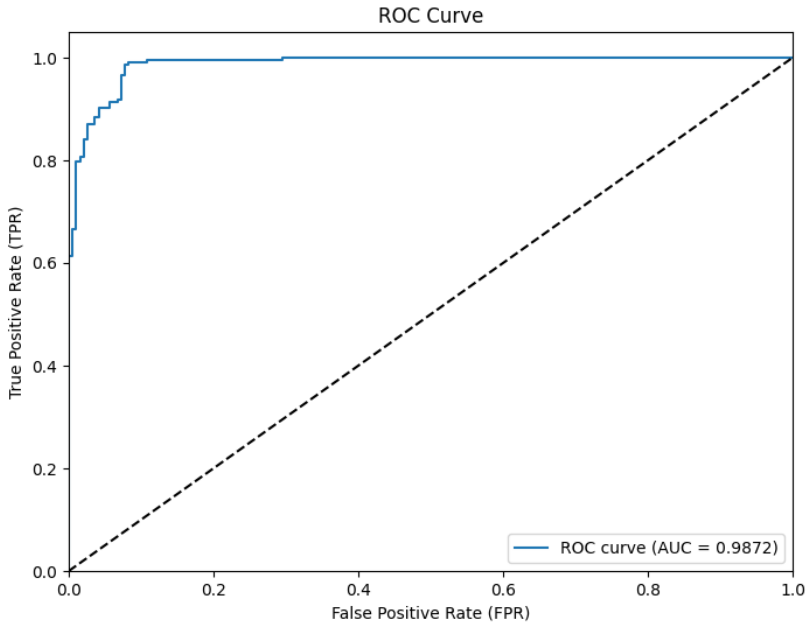
12 lentelė. Mašininio mokymosi modelių rezultatų palyginimas – bendras tikslumas (treniravimo imtis)

Treniravimo / testavimo imčių santykis	**Random Forest**	**ADA_Boost**	**XG_Boost**
80/20	0.963	0.983	0.996
75/25	0.964	0.980	0.994
70/30	0.967	0.984	0.993

Galima matyti, kad visi modeliai treniravimo imtį klasifikavo šiek tiek geriau nei testavimo imtį (11 lentelė. ir 12 lentelė.), visgi gauti skirtumai siekia apie 2%, nei vienas modelis nespėlioja tobulai. Galima teigti, kad suderinus modelių hiperparametrus, modeliai neprisitaikė prie treniravimo imčių ir buvo išvengta persimokymo.

4.2.5. Vizualus klasifikavimo modelio įvertinimas

Vizualiai modelio efektyvumas vertinamas pasitelkiant ROC kreivę. Ši kreivė nurodo kaip keičiant klasifikavimo slenkstį (angl. *Classification threshold*) kinta modelio gebėjimas teisingai klasifikuoti teigiamus ir neigiamus atvejus (35 pav.).



35 pav. Atsitiktinio miško modelio veikimo charakteristikos kreivė

Galima matyti:

- Ašis X: klaidingai teigiamos prognozės, lyginant su visais neigiamais atvejais.

$$FPR = \frac{FP}{(FP + TN)}$$

Čia *FP* (angl. *False positives*) yra klaidingai teigiami, o *TN* (angl. *True negatives*) yra tikrai neigiami atvejai. *FPR* (angl. *False positive rate*) taip pat žinomas kaip klaidingo pavojaus dažnis.

- Ašis Y: teisingai teigiamų prognozių dalis iš visų teigiamų atvejų, dar vadinama specifiškumu.

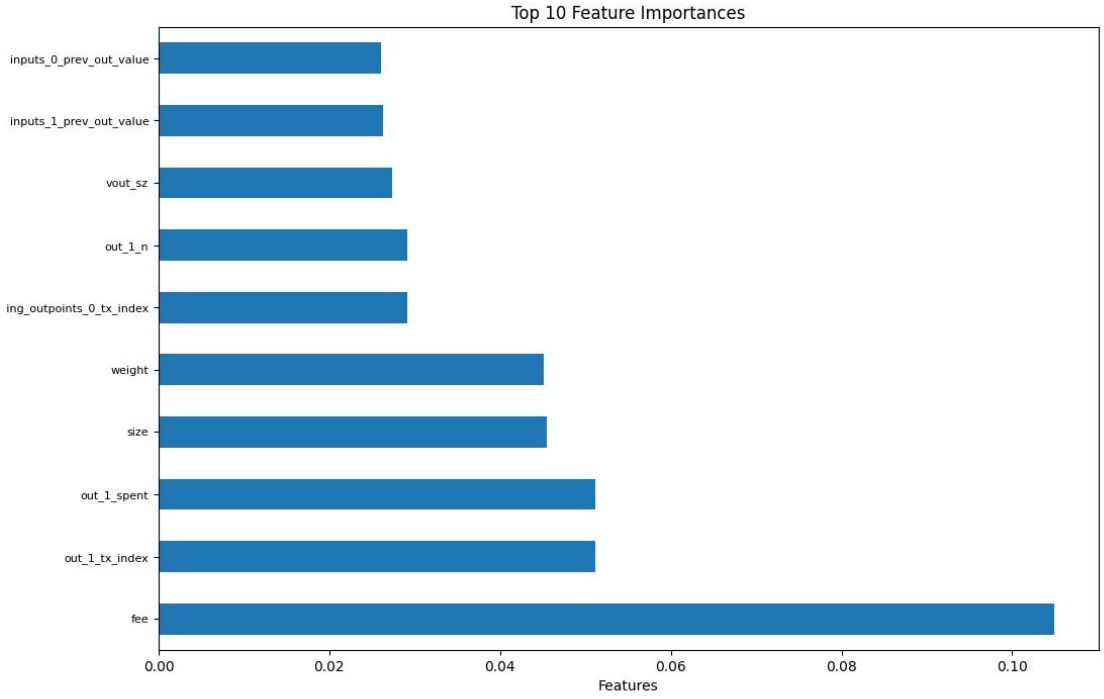
$$TPR = \frac{TP}{(TP + FN)}$$

Čia TP (angl. *True positives*) yra tikrai teigiami, o FN (angl. *False negatives*) yra klaidingai neigiami atvejai.

Plotas po šia kreive yra skaitinis rodiklis, kurio reikšmė priklauso intervalui [0;1]. Reikšmė 0.5 reikštų, kad modelis atitinka atsitiktinį klasifikatorių, tuo tarpu 1 atitiktų idealų klasifikatorių. Konkrečiu atveju plotas po kreive yra 0.9872, tai reiškia, kad modelis labai efektyvus atskiriant skirtingas klases.

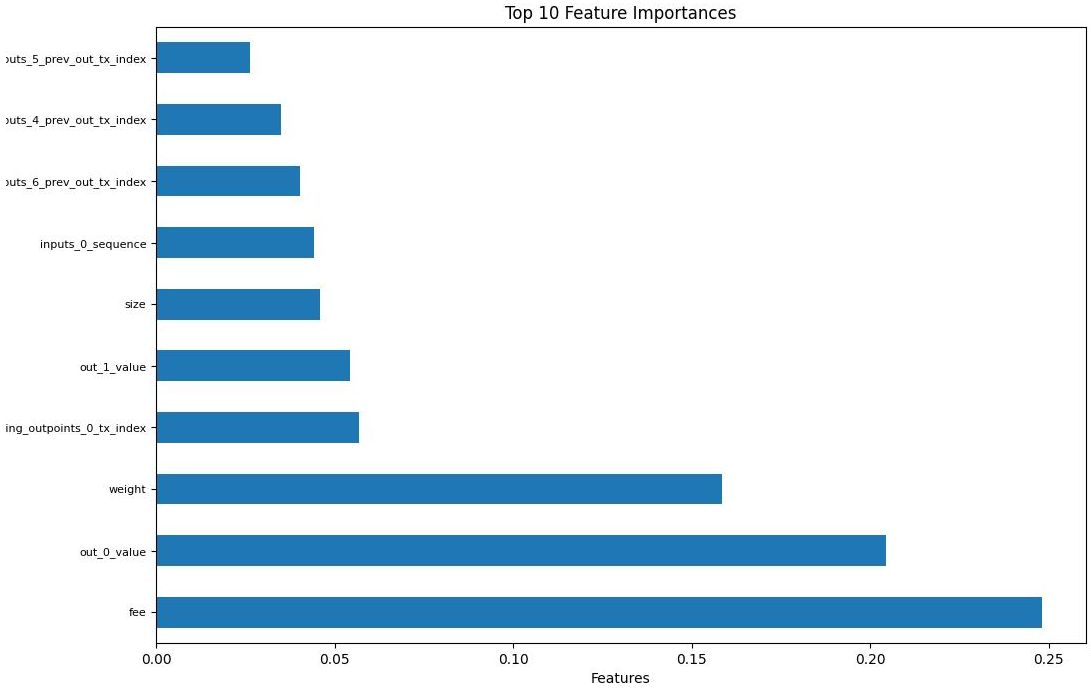
4.2.6. Svarbiausi požymiai

Ištreniravus modelius su atrastais geriausiai modelių hiperparametrais atliekama svarbiausių požymių analizė.



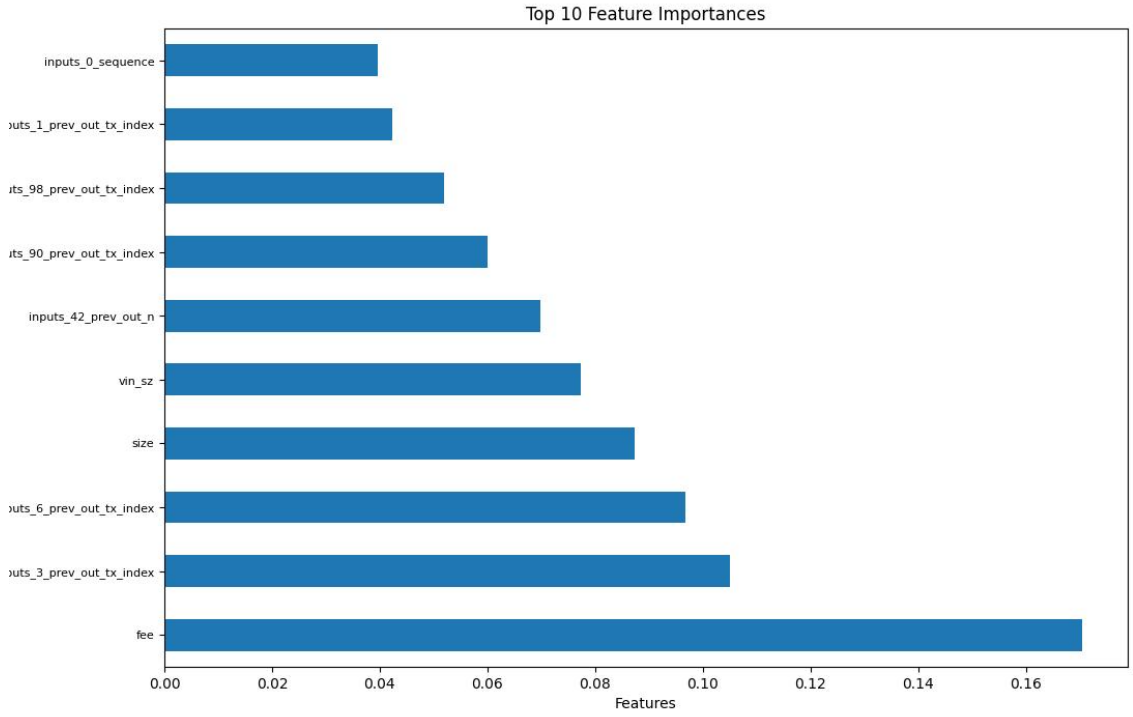
36 pav. Atsitiktinio miško svarbiausi požymiai

Atsitiktinio miško svarbiausių požymių grafike (36 pav.) matyti, kad finansinės operacijos mokestis yra svarbiausias požymis atliekant klasifikavimo uždavinį, maždaug du kartus svarbesnis už antroje ir trečioje vietoje esančius požymius.



37 pav. *ADABoost* modelio svarbiausi požymiai

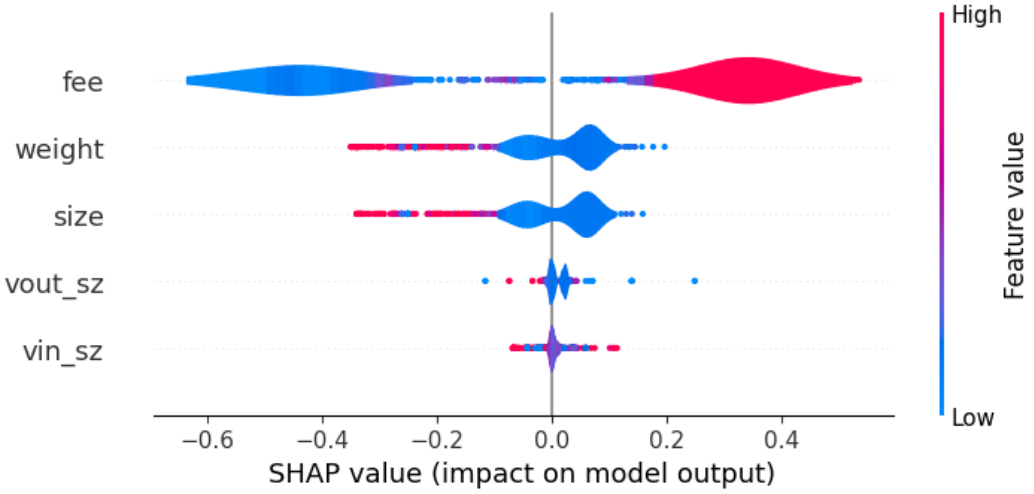
ADA Boost modelio svarbiausias požymis taip pat mokestis už finansinę operaciją, visgi nedaug atsilieka ir antroje bei trečioje vietoje pagal svarbumą esantys pirmosios išeigos reikšmė (*out_0_value*) ir svoris (*weight*) atitinkamai (37 pav.).



38 pav. *XGBoost* modelio svarbiausi požymiai

Visų 3 modelių svarbiausias požymis yra tas pats – finansinės operacijos mokestis, visgi galima pastebėti, kad *ADA Boost* modelyje jo svoris siekia ~0.25, tuo tarpu *XGBoost* ir atsitktinio miško ~0.16 ir ~0.10 atitinkamai (36 pav. , 37 pav. , 38 pav.).

Toliau su modelio požymiais atliekama *SHAP* (angl. *Shapley Additive exPlanations*) analizė (39 pav.).



39 pav. *Shapley* modelio požymių svarbos grafikas

Grafikas atvaizduoja tik didžiausią poveikį klasifikavimui turinčius požymius bei atskleidžia, kaip kiekvienas duomenų rinkinio požymis prisideda prie mašininio modelio, nustatančio finansinių

operacijų legalumą išvesties. Požymiai esantys viršuje yra patys svarbiausi, kuo didesnis SHAP vertės diapazonas, tuo požymis svarbesnis.

Šiuo atveju svarbiausi požymiai:

- Mokestis (angl. *fee*): Svarbiausias požymis. Aukštesnės mokesčio reikšmės (raudona spalva) dažniausiai turi teigiamą *SHAP* reikšmę, o žemesnės mokesčio reikšmės (mėlyna spalva) dažniausiai turi neigiamą *SHAP* reikšmę. Didelis mokestis gali būti susijęs su skuba atlikti finansines operacijas, arba siuntėjas nori suteikti didesnį prioritetą tam, kad finansinės operacijos būtų greičiau įtrauktos į bitcoin bloką. Nors pats mokestis savaime nėra nelegalumo indikatorius, didelė jo vertė gali būti susijusi su didelės vertės finansinėmis operacijomis, kurios gali būti tiek legalios, tiek nelegalios. Mažas mokestis reiškia kad finansinė operacija nėra skubi, siuntėjas linkęs taupyti, taip pat tai gali būti automatizuotos didelio masto finansinės operacijos, kurios gali būti naudojamos kaip bandymai „išplauti“ mažas sumas.

- Dydis (angl. *size*) ir svoris (angl. *weight*): stipriai koreliuoti požymiai, dydis ir svoris yra susiję su finansinės operacijos sudėtingumu – dydžiu baitais ir įvairiais komponentais. Didelio svorio operacijos gali reikšti, kad pinigai yra konsoliduojami iš daugelio šaltinių arba skaidomi į daug adresų. Tokie veiksmai gali būti būdingi tiek legalioms (pvz., biržų operacijos), tiek nelegalioms veikoms (pvz., pinigų plovimas, kai stengiamasi sumaišyti lėšų kilmę). Tuo tarpu mažos požymių reikšmės nurodo, kad operacija buvo tiesioginis pervedimas tarp dviejų šalių.

- Išvesčių kiekis (angl. *vout_sz*) ir įvesčių kiekis (angl. vin_sz): Didelis kiekis išvesčių reiškia, kad pinigai yra skaidomi į daugybę skirtingų adresų, tuo tarpu didelis kiekis įvesčių reiškia, kad pinigai yra surenkami iš daugybės skirtingų šaltinių. Didelė vieno ar kito požymio reikšmė gali potencialiai indikuoti maišytuvų naudojimą, kas padaro finansinę operaciją įtartina.

Reikėtų paminėti, kad modelis nagrinėja požymių kombinacijas ir vienas atskiras požymis nebūtinai padaro finansinę operaciją nelegalia.

Išvados

Magistro darbe buvo sukurtas *bitcoin* blokų grandinės finansinių operacijų analizavimo įrankis, gebantis klasifikuoti realaus laiko finansines operacijas bei paaiškinti savo sprendimus. Geriausius rezultatus pasiekė *XGBoost* architektūros modelis. Darbo metu prieitos išvados:

1. Atlikus skaitmeninės kriminalistikos bei jos taikymo blokų grandinių technologijos srityje analizę patvirtinta, kad skaitmeninėje kriminalistikoje trūksta mašininio mokymosi modelių kurie paspartintų skaitmeninės analizės procesus, egzistuojantiems mašininio mokymosi metodams taikomiems skaitmeninėje kriminalistikoje trūksta aiškumo, paaiškinamumo, kas apsunkina jų taikymą teisminiame procese.

2. Atlikus viešų kriptovaliutų finansinių operacijų duomenų rinkinių analizę nuspęsta, kad tyrimui bus naudojamas duomenų rinkinys – *Elliptic* paskelbto duomenų rinkinio su etiketėmis bei viešai prieinamų duomenų gaunamų iš *blockchain.info* kombinacija. Nesubalansuoto duomenų rinkinio problemą nuspręsta spręsti atsitiktinai pašalinant didesnės klasės stebinius, taip suvienodinant klasių stebinių kiekius rinkinyje.

3. Realizuojant prototipą buvo susidurta su duomenų nutekėjimo problema, kuomet duomenų normalizatorius buvo apmokytas su visais duomenimis, tai išspręsta kuriant normalizatorių išskirtinai naudojant tik treniravimo duomenis, užtikrinant, kad testavimo imtis liktų nepriklausoma. Ištreniruotų modelių klasifikavimo sprendimams aiškinti pasirinkta naudoti *SHAP* analizė.

4. Eksperimento metu aptikta, kad nelegalioms finansinėms operacijoms *bitcoin* kriptovaliutos blokų grandinėje aptikti labiausiai tinka *XGBoost* mašininio mokymosi modelis, geriausi hiperparametrai algoritmui yra: medžių skaičius – 150, mokymosi greitis 0.01. Ištreniruotas modelis nelegalias finansines operacijas klasifikuoja kaip legalias dažniau, nei legalias kaip nelegalias. Svarbiausi modelio požymiai yra finansinės operacijos mokestis, taip pat didelę įtaką daro įvesčių, išvesčių į finansinę operaciją skaičius bei finansinės operacijos dydis.

Literatūros sąrašas

1. AJIN S - AJITH GS Bitcoin security - Anti-Dust Attack. [interaktyvus]. 2022. [žiūrėta 2025-04-23]. Prieiga per internetą: <https://zenodo.org/doi/10.5281/zenodo.6383689>.

2. AKCORA, C.G. ir kt. Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota. In *WIREs Data Mining and Knowledge Discovery* . 2022. Vol. 12, no. 1, p. e1436.

3. AKHTAR, M. - FENG, T. Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment. In *EAI Endorsed Transactions on Creative Technologies* . 2022. p. 174089.

4. AKINBI, A. ir kt. A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. In *Forensic Science International: Digital Investigation* . 2022. Vol. 42–43, p. 301470.

5. AMATO, F. ir kt. Analyse digital forensic evidences through a semantic-based methodology and NLP techniques. In *Future Generation Computer Systems* . 2019. Vol. 98, p. 297–307.

6. CLAIN [interaktyvus]. .2019. Prieiga per internetą: <https://www.kaggle.com/datasets/alexbenzik/deanonymized-995-pct-of-elliptic-transactions>.

7. DUNSIN, D. ir kt. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. In *Forensic Science International: Digital Investigation* . 2024. Vol. 48, p. 301675.

8. ELLIPTIC [interaktyvus]. .2019. Prieiga per internetą: <https://www.kaggle.com/datasets/ellipticco/elliptic-data-set>.

9. FOLEY, S. ir kt. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? In *The Review of Financial Studies* . 2019. Vol. 32, no. 5, p. 1798–1853.

10. HALL, S.W. ir kt. Explainable artificial intelligence for digital forensics. In *WIREs Forensic Science* . 2022. Vol. 4, no. 2, p. e1434.

11. HILMAND, K. ir kt. A survey of machine learning applications in digital forensics. In *Trends in Computer Science and Information Technology* . 2021. p. 020–024.

12. HSIEH, S.-F. - BRENNAN, G. Issues, risks, and challenges for auditing crypto asset transactions. In *International Journal of Accounting Information Systems* . 2022. Vol. 46, p. 100569.

13. YAACOUB, J.-P.A. ir kt. Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. In *Internet of Things* . 2022. Vol. 19, p. 100544.

14. KARIE, N.M. ir kt. Diverging deep learning cognitive computing techniques into cyber forensics. In *Forensic Science International: Synergy* . 2019. Vol. 1, p. 61–67.

15. KEBANDE, V.R. ir kt. Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. In *Forensic Science International: Reports* . 2020. Vol. 2, p. 100122.

16. LI, Y. ir kt. Dissecting Ethereum Blockchain Analytics: What We Learn from Topology and Geometry of Ethereum Graph. In [interaktyvus]. 2019. [žiūrėta 2023-01-15]. Prieiga per internetą: <https://arxiv.org/abs/1912.10105>.

17. LI, M. ir kt. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. In *Future Generation Computer Systems* . 2021. Vol. 115, p. 406–420.

18. LIANG, J. ir kt. Targeted Addresses Identification for Bitcoin with Network Representation Learning. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)* [interaktyvus]. Shenzhen, China: IEEE, 2019. p. 158–160. [žiūrėta 2022-11-27]. Prieiga per internetą: <https://ieeexplore.ieee.org/document/8823249/>.

19. LIN, C.-Y. ir kt. A Systematic Review of Detecting Illicit Bitcoin Transactions. In *Procedia Computer Science* . 2022. Vol. 207, p. 3217–3225.

20. LINAS POCIUS [interaktyvus]. Prieiga per internetą: <https://github.com/Linupo/MBD>.

21. LORENZ, J. ir kt. 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]. New York New York: ACM, 2020. p. 1–8. [žiūrėta 2022-11-21]. Prieiga per internetą: <https://dl.acm.org/doi/10.1145/3383455.3422549>.

22. LTEC Metodinės rekomendacijos informacinių technologijų ir mobiliųjų įrenginių ekspertinių tyrimų užsakovams. [interaktyvus]. 2025. [žiūrėta 2025-04-12]. Prieiga per internetą: <https://ltec.lrv.lt/lt/veiklos-sritys/ekspertiniu-tyrimu-atlikimas/>.

23. MOHAMMAD, R.M.A. - ALQAHTANI, M. A comparison of machine learning techniques for file system forensics analysis. In *Journal of Information Security and Applications* . 2019. Vol. 46, p. 53–61.

24. NERURKAR, P. Illegal activity detection on bitcoin transaction using deep learning. In *Soft Computing* . 2023. Vol. 27, no. 9, p. 5503–5520.

25. PONCE-BOBADILLA, A.V. ir kt. Practical guide to SHAP analysis: Explaining supervised machine learning model predictions in drug development. In *Clinical and Translational Science* . 2024. Vol. 17, no. 11, p. e70056.

26. REN, Y.-S. ir kt. Past, present, and future of the application of machine learning in cryptocurrency research. In *Research in International Business and Finance* . 2022. Vol. 63, p. 101799.

27. RETZLAFF, C.O. ir kt. Post-hoc vs ante-hoc explanations: xAI design guidelines for data scientists. In *Cognitive Systems Research* . 2024. Vol. 86, p. 101243.

28. ROSENQUIST, H. ir kt. On the Dark Side of the Coin: Characterizing Bitcoin Use for Illicit Activities. In RICHTER, P. ir kt.Sud. *Passive and Active Measurement* [interaktyvus]. Cham: Springer Nature Switzerland, 2024. p. 37–66. [žiūrėta 2025-05-04]. ISBN 978-3-031-56251-8 Prieiga per internetą: <https://link.springer.com/10.1007/978-3-031-56252-5_3>.

29. SOLANKE, A.A. Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. In *Forensic Science International: Digital Investigation* . 2022. Vol. 42, p. 301403.

30. VENČKAUSKAS, A. ir kt. Machine Learning in Money Laundering Detection Over Blockchain Technology. In *IEEE Access* . 2025. Vol. 13, p. 7555–7573.

31. WEBER, M. ir kt. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. [interaktyvus]. 2019. [žiūrėta 2022-11-21]. Prieiga per internetą: <https://arxiv.org/abs/1908.02591>.

32. WU, J. ir kt. Analysis of cryptocurrency transactions from a network perspective: An overview. In *Journal of Network and Computer Applications* . 2021. Vol. 190, p. 103139.

33. ZAFAR, M.R. - KHAN, N. Deterministic Local Interpretable Model-Agnostic Explanations for Stable Explainability. In *Machine Learning and Knowledge Extraction* . 2021. Vol. 3, no. 3, p. 525–541.

34. Blockchain explorer. [interaktyvus]. Prieiga per internetą: <https://www.blockchain.com/explorer>.

35. Chainalysis. [interaktyvus]. Prieiga per internetą: <https://www.chainalysis.com/>.

36. Elliptic Lens Overview. [interaktyvus]. Prieiga per internetą: <https://www.elliptic.co/platform/lens>.

Priedai

1 priedas. Parašyto straipsnio „Machine Learning in Money Laundering Detection Over Blockchain Technology“ santrauka[30]

Kartu su KTU dėstytojais kriptovaliutų operacijų analizės tematika išleidome straipsnį skaitmeninėje straipsnių duombazėje *IEEE Explore* pavadinimu *Machine Learning in Money Laundering Detection Over Blockchain Technology*. Straipsnis apžvelgia pinigų plovimo problemą blokų grandinėje ir nagrinėja mašininio mokymosi panaudojimą šios veiklos aptikimui, o tai tiesiogiai atliepia ir šio baigiamojo darbo tikslus. Straipsnyje taip pat išsamiai apžvelgtos problemos kylančios dėl didėjančio kriptovaliutų populiarumo ir blokų grandinės technologijos ypatybių, leidžiančių greitai ir anonimiškai pervesti lėšas, nagrinėjami įvairūs pinigų plovimo etapai, ypatingą dėmesį skiriant maskavimo procesui, kuriame nusikalstamos lėšos yra slepiamos per sudėtingus finansinių operacijų tinklus.

Pagrindinis straipsnio tikslas įvertinti mašininio mokymosi metodų potencialą aptinkant nelegalias finansines operacijas blokų grandinių tinkluose. Straipsnyje aptariami duomenų apdorojimo būdai, būtini norint paruošti blokų grandinių finansinių operacijų duomenis algoritmams, tada dokumente analizuojamas įvairių klasifikavimo algoritmų efektyvumas, aptariant jų privalumus bei trūkumus nelegalių *bitcoin* finansinių operacijų kontekste.

Straipsnyje pateikti rezultatai parodė, kad mašininis mokymas gali būti vertingas įrankis automatizuojant sprendimus naudojamus kovai prieš nusikalstamas veiklas blokų grandinėse. Konkrečiai straipsnyje bei baigiamajame darbe nagrinėti metodai pademonstravo, kad tam tikri dirbtinio intelekto modeliai gali pasiekti itin aukštą tikslumą ir pasitarnauti teisėsaugai klasifikuojant finansines operacijas kaip teisėtas arba įtartinas, taip sumažinant žmogiškųjų klaidų skaičių bei žmogiškųjų išteklių poreikį reikalingą atlikti sudėtingas blokų grandinių analizes[30].