Rug pull -huijausten moniulotteinen analysointi DeFi-ekosysteemin hajautetuissa pörsseissä

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Maaliskuu 2026
Tiitus Heikkinen

TURUN YLIOPISTO
Tietotekniikan laitos

Tiitus Heikkinen: Rug pull -huijausten moniulotteinen analysointi DeFi-ekosysteemin hajautetuissa pörsseissä

TkK-tutkielma, 22 s.
Tietotekniikka
Maaliskuu 2026

Rug pull -huijaukset ovat kryptovaluutoilla toteutetun hajautetun rahoituksen eli DeFi-ekosysteemin yleisin huijausmuoto, joissa sijoittajat menettävät vuosittain huomattavia rahasummia. Rug pull -huijauksissa pahantahtoiset kehittäjät luovat DeFi-projekteja, esimerkiksi älysopimuksina Ethereum-lohkoketjuun, tarkoituksena huijata sijoittajia. Tässä tutkimuksessa keskitytään tarkastelemaan DeFi-ympäristössä tapahtuvien niin sanottujen rug pull -huijausten tunnuspiirteitä ja sitä, millä eri tavoin ja missä vaiheessa huijaustarkoitukseen luodun DeFi-projektin elinkaarta voidaan näitä tunnuspiirteitä tunnistaa. Teknisestä näkökulmasta rug pull -huijausten tunnuspiirteitä ovat älysopimuksen haavoittuvainen tai haitallinen koodi ja sitä pyritään analysoimaan esimerkiksi tavukoodista johdetulla mallilla ja Datalog-säännöillä. Taloudellisesta näkökulmasta likviditeetin poikkeavat muutokset, kuten äkilliset poistot, kaupankäyntitapahtumien poikkeavuudet ja keskittynyt tokenin omistajuus osoittavat riskiä rug pull -huijaukselle. Näitä voidaan esimerkiksi analysoida Herfindahl–Hirschman-indeksillä ja koneoppimisella. Sosiaalisesta näkökulmasta aggressiivinen DeFi-projektin markkinointi sosiaalisessa mediassa tai tokenin brändin kopiointi viittaavat rug pull -huijauksen tunnuspiirteisiin. Sosiaalisia tunnuspiirteitä voidaan pyrkiä tunnistamaan tekoälyn menetelmin. Tutkielman keskeisenä johtopäätöksenä todetaan, että rug pull -huijauksen riskiä ei voida havaita vain yhdestä näkökulmasta tarkasteltuna. Sen sijaan havainnoinnin pitää olla kokonaisvaltaista ja ulottua myös täysin lohkoketjuteknologian ulkopuolelle parhaan analyysin tuottamiseksi.

Asiasanat: rug pull, lohkoketju, kryptovaluutta, defi

Sisällys

1 Johdanto

Hajautettu rahoitus (engl. *decentralized finance*, DeFi) on muodostunut merkittäväksi sovellusalueeksi lohkoketjuteknologiassa. Toukokuussa 2025 DeFi-projekteihin lukittu rahallinen kokonaisarvo (engl. *total value locked*, TVL) saavutti 250 miljardin rajapyykin [1]. Tärkeitä DeFi-palveluita ovat esimerkiksi lainaaminen ja kryptovaluutan muuntaminen toiseen [2]. DeFi-ekosysteemi tarjoaa kaupankäyntialustoja, joissa osassa käyttäjät voivat vaihtaa eri kryptovaluuttoja keskenään ja pitää yllä likviditeettiä. Osassa DeFi-ekosysteemin kaupankäyntialustoista käyttäjät voivat puolestaan lainata ja ottaa lainaksi kryptovaluuttoja [2]. Valuutanvaihtopalveluita tarjoavat hajautetut pörssit (engl. *decentralized exchange*, DEX). Ne toimivat joko tilauskannan (engl. *order book*) tai automaattisten kaupankäyntiin keskittyneiden älysopimusten (engl. *automated market maker*, AMM) avulla.

AMM-pohjaiset DEX-alustat hyödyntävät likviditeettipooleja (engl. *liquidity pools*) mahdollistaakseen varojen vaihdon hajautetuissa pörsseissä ilman suoranaista vastapuolta, kuten erillistä ostajaa tai myyjää. Likviditeettipoolit toimivat kuin valuuttakurssit, joissa on valuuttaparit. Toisin kuin perinteisissä valuuttakursseissa, joissa keskitetyt tahot tarjoavat likviditeetin, likviditeettipooleissa kuka vain, joka omistaa likviditeettipoolin hyväksymiä kryptovaluuttoja, voi tarjota siihen likviditeettiä. Samalla AMM-pohjaiset DEX-alustat ovat helpottaneet tyypillisiä kryptovaluuttahuijauksia, kuten *rug pull* -huijausta. Rug pull -huijauksia voi tapahtua kryptovaluutoissa muutenkin, mutta viime vuosina AMM-mekanismien tulon myö-

tä ne suurimmaksi osaksi ovat tapahtuneet AMM-pohjaisilla DEX-alustoilla. Tässä tutkielmassa perehdytään AMM-pohjaisilla DEX-alustoilla tapahtuviin rug pull -huijauksiin, mutta esiteltyjä huijausten tunnistusmenetelmiä voi hyödyntää osittain myös muissa kryptovaluuttoihin liittyvissä rug pull -huijauksissa.

Tyypillinen AMM-pohjaisella DEX-alustalla tapahtuva rug pull -huijaus noudattaa usein tietynlaista kaavaa. Ensiksi DeFi-projektin pahantahtoinen kehittäjä luo uuden tokenin, jonka kautta varhaiset sijoittajat voivat pian osallistua projektin kehitykseen ostamalla tokenia. Tämän jälkeen kehittäjä listaa jollakin AMM-pohjaisella DEX-alustalla tokenin vaihdettavaksi vastinpariin, joka on yleensä jokin tunnettu ja arvokas token. Toisin sanoen kehittäjä luo likviditeettipoolin, johon hän sijoittaa sekä luomaansa tokenia, että tunnettua tokenia. Likviditeettipooliin sijoittamistaan varoista kehittäjä saa itselleen LP-tokeneita (engl. *liquidity provider tokens*), jotka kehittäjä voi myöhemmin lunastaa takaisin, tyhjentäen likviditeettipoolin molemmat tokenit omaan kryptovaluuttalompakkoonsa. Kun likviditeettipooli on luotu, sijoittajia houkutellaan ostamaan tokenia, eli vaihtamaan arvokasta tokenia tähän uuteen kehittäjän luomaan tokeniin. Kun token on kerännyt tarpeeksi sijoituksia ja token on nostanut arvoaan vastinpariinsa nähden, kehittäjä poistaa likviditeettipoolin likviditeetin vaihtamalla LP-tokeninsa takaisin likviditeettipoolin tokeneihin.

Tämän tutkielman tavoitteena on selkeyttää rug pull -huijauksia kokonaisuutena ja lisäki selvittää millaisia menetelmiä rug pull -huijausten tunnistamisessa voitaisiin hyödyntää. Aiemmat tutkimukset sisältävät menetelmiä rug pull -huijauksen analysointiin ja tässä tutkielmassa syvennytään aiemmin esiteltyjen työkalujen taustalla oleviin menetelmiin. Tunnistusmenetelmät sekä rug pull -huijausten tunnuspiirteet jaotellaan teknisiin, taloudellisiin ja sosiaalisiin osa-alueisiin. Jaottelu paljastaa, etteivät rug pull -huijaukset ole vain tekninen ongelma älysopimuksessa tai taloudellinen epätasapaino tokenin haltijuudessa, vaan sijoitajia myös houkutellaan mukaan

huijauksiin esimerkiksi sosiaalisessa mediassa. Täten rug pull -huijaus on moniulotteinen ilmiö ja tarvitsee laaja-alaista analysointia, jotta mahdollinen huijaus tunnistetaan parhaiten.

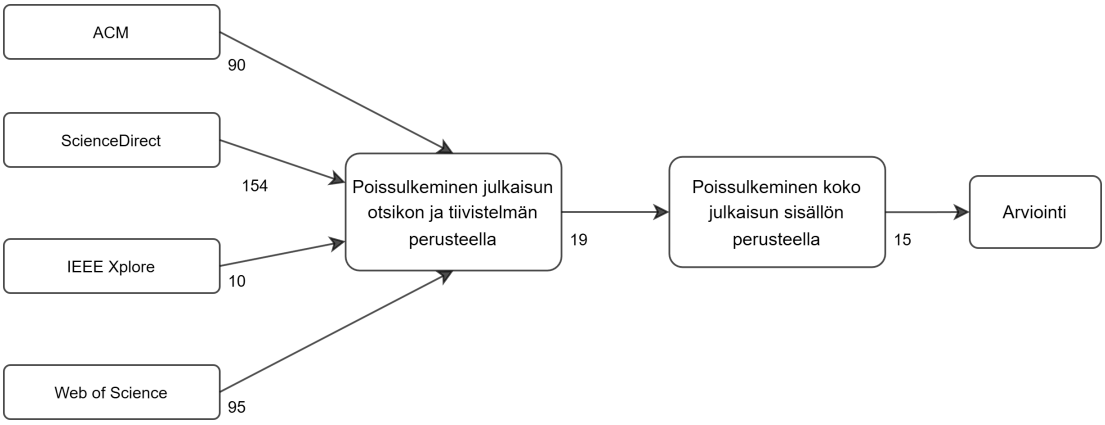
Tutkielmalle asetetut tutkimuskysymykset ovat seuraavat:

TK1: Mitkä ovat rug pull -huijauksen tyypilliset tunnusmerkit?

TK2: Millä tunnistusmenetelmillä rug pull -huijaukset tunnistetaan parhaiten?

Tutkielma on toteutettu kirjallisuuskatsauksena aiheeseen. Toisessa luvussa pohjustetaan aihetta taustatiedoilla lohkoketjuteknologian toiminnasta ja erilaisista lohkoketjuista. Kolmas luku kertoo DeFi-ekosysteemistä ja siihen liittyvistä erilaisista kryptovaluuttahuijauksista. Neljännessä luvussa esitellään viimeaikaisessa tieteellisessä kirjallisuudessa esiteltyjä työkaluja ja menetelmiä rug pull -huijausten tunnistamisen avuksi ja älysopimusten analysoimiseksi. Viides luku vertailee tuloksia näiden tunnistustyökalujen välillä. Tutkielman päättävässä kuudennessa luvussa vastataan tutkimuskysymyksiin ja pohditaan jatkotutkimusaiheita.

Tutkimuksessa käytetään julkaisuja neljästä eri hakukannasta: ACM (Association for Computer Machinery) Digital Library, IEEE (Institute of Electrical and Electronics Engineers) Xplore, Web of Science ja ScienceDirect. Tiedonhakua varten käytettiin edellä mainittuihin hakukantoihin seuraavaa hakulausetta:
("blockchain"OR "defi"OR "smart contract") AND ("rug pull"OR "pump and dump"OR "exit scam") AND ("analysis"OR "detection"OR "anomaly")
Hakukannoissa valittiin vain vuosien 2021 ja 2025 välillä julkaistut aineistot tarkasteltavaksi. Kuvan 1.1 mukaisesti julkaisuja karsittiin otsikon ja tiivistelmän perusteella ja lopuksi myös koko julkaisun sisällön perusteella. Numerot kuvaavat kuinka monta julkaisua on tiedonhaun eri vaiheissa otettu huomioon. Alussa hakukantojen vieressä numerot kuvaavat kuinka monta hakutulosta hakukannasta löytyi hakulauseella ja vuosilukusuodatuksen kanssa.



Kuva 1.1: Tiedonhakuprosessi

2 Kryptovaluuttojen nykytila

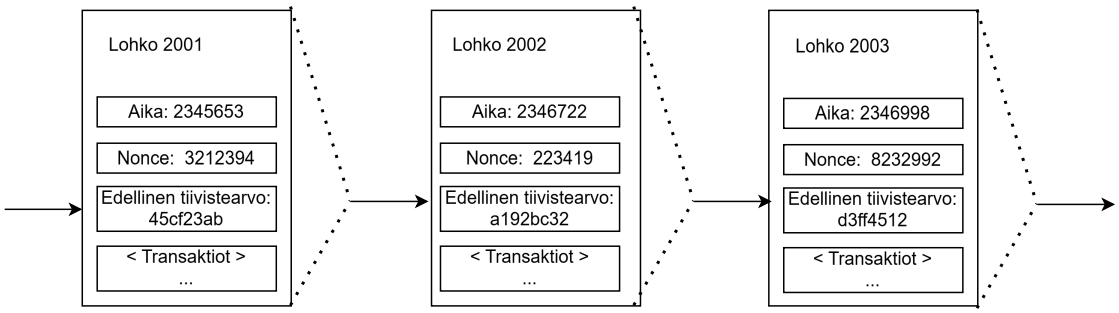
2.1 Lohkoketjun toimintaperiaate

Alkujaan Bitcoinin myötä tunnetuksi tullut termi *lohkoketju* tarkoittaa jaettua pääkirjaa (engl. *ledger*) hajautetussa ympäristössä. Tarkemmin sanottuna tämä pääkirja on liuta lohkoja, jotka kukin sisältävät listan transaktioita, esimerkiksi rahansiirtotapahtumia. Nämä lohkot linkittyvät toisiin peräkkäin muodostaen ketjumaisen rakenteen. Kun uusi lohko on louhittu ja se on hyväksytty muiden louhijoiden (engl. *miners*) taholta konsensusprotokollan mukaisesti kelvolliseksi, lisätään lohko lohkoketjun jatkeeksi. Jokaisella louhijalla on oma kopio yhteisestä pääkirjasta taaten samalla, että lohkoketjuun tallennettu tieto pysyy hajautettuna ja muuttumattomana. Tämä tarkoittaa, että mikään taho ei voi muuttaa tai poistaa tietoa, kun se on kerran tallennettu lohkoketjuun.

Työn todiste (engl. *Proof of Work*, PoW) -pohjaisissa lohkoketjuissa, kuten Bitcoinissa ja alun perin Ethereumissa, uuden lohkon löytänyt louhija on saanut päättää mitä transaktioita lohkoon kirjoitetaan. Toisin sanoen louhija päättää, mitkä rahansiirtotapahtumat tulevat voimaan, kun muut verkon jäsenet, eli muut louhijat, ovat vahvistaneet lohkon oikeellisuuden. Uuden lohkon louhija ei voi sisällyttää kaikkia transkatioita lohkoon lohkon rajallisen koon puolesta ja suosii yleensä transaktioita, jotka tuovat louhijalle suurimmat lohkopalkkiot. [3]

Uusi lohko syntyy, kun löydetään jokin satunnainen luku, *nonce*, joka yhdessä

ajan, transaktioiden ja edellisen lohkon tiivistearvon kanssa ajettuna tiivistefunktion läpi tuottaa sallitun tiivistearvon. Sallittu tiivistearvo on muiden verkon jäsenten kanssa sovitun arvoalueen rajoissa oleva tiivistearvo. Käytännössä kryptovaluutan louhiminen on vain lukuisien tiivistearvojen tuottamista nopealla tahdilla. Kuvassa 2.1 esitetään kuinka uudet lohkot linkittyvät aikaisempiin aikaisempien lohkojen tiivistearvojen (engl. *hash*) kautta.



Kuva 2.1: Lohkojen välinen yhteys

2.2 Ethereum

Lohkoketjuteknologian kehittymisen myötä kehittäjät ovat alkaneet tarkastella mahdollisuuksia toteuttaa hajautettuja sovelluksia, kuten pankkitoimintoja tarjoavia palveluja, lohkoketjujen avulla. Tämän kehityksen myötä on syntynyt esimerkiksi Ethereum-lohkoketju [4] ja sitä kautta käyttöön tulleet älysopimukset [5].

Myös Bitcoin-lohkoketjun yhteyteen yritettiin rakentaa älysopimuksia. Turing-täydellisen ohjelmointikielen puuttuminen ja tilattomuus (engl. *statelessness*) tekivät Bitcoinissa toimivien älysopimusten luonnista haastavaa. Vuonna 2015 käynnistetty Ethereum-lohkoketju kehitettiin sen kryptovaran kuvauksen [6] (engl. *white-paper*) mukaan ratkaisemaan Bitcoinissa havaitut ongelmat. Siinä missä Bitcoin on pelkkä valuutta, Ethereum pyrkii tuomaan perinteisen finanssialan palvelut, kuten lainaamisen ja valuuttamuunnokset, hajautettuun ja keskittämättömään verkkoon.

3 Rug pull -huijaukset DeFi-projekteissa

3.1 DeFi-ekosysteemi ja sen rakenne

Ymmärtääkseen tokenien toimintaa, on välttämätöntä ymmärtää niiden ympärillä toimivaa DeFi-ekosysteemiä, eli kaikkea sitä, mitä käsite *DeFi* pitää sisällään. Xue ym. [7] esittelee tutkimuksessaan erilaisia DeFi-sovellusluokkia lohkoketjussa. Näihin sovellusluokkiin kuuluvat:

- lohkoketjujen väliset sillat (engl. *cross chain bridge*): mahdollistavat varojen siirtämisen lohkoketjusta toiseen
- hajautetun kaupankäynnin välineet (engl. *decentralized intermediaries and products*): tarjoavat finanssialan palveluita, kuten lainaus- ja vakuuspalveluita
- hajautetut pörssit: mahdollistavat tokenien kaupankäynnin ilman keskitettyjä, kolmansia osapuolia
- tokenit (engl. *token system*): usein ERC-20-standardiin perustuvat kryptotokenit
- oraakkelit (engl. *oracle*): välittävät älysopimuksille dataa lohkoketjujen ulkopuolelta, reaalimaailmasta

3.2 ERC-20-standardi

Suurin osa Ethereum-alustan päälle rakennetuista tokeneista noudattavat *Ethereum Request for Comments 20* -standardia (ERC-20) [4]. ERC-20-standardissa määritellään tietyt funktiot, jotka jokaisen tämän standardin mukaisen tokenin pitää toteuttaa. Näitä funktioita ovat muun muasssa *transfer*, *approve* ja *totalSupply* [2]. Edellisten funktioiden lisäksi tokenin kehittäjällä on mahdollisuus ohjelmoida muita funktioita tokenin älysopimukseen. Tässä piilee mahdollisuus väärinkäytöksille, koska kehittäjien on mahdollista piilottaa älyopimukseen myös haitallisia funktioita, kuten niin sanottuja minttausfunktioita eli uusien tokenien luonti -funktioita tai siirtorajoituksia. Lin ym. [8] ja Zhou ym. [9] esittelevät menetelmiä, jotka tunnistavat haitallisia mekanismeja, kuten *modifyBalance-, blacklist-, sell limit-* ja *hidden mint* -funktioita.

3.3 Hajautetut pörssit

Hajautetut pörssit, eli DEX:t, ovat yksi DeFi-protokollan kategoria [7, 10]. DEX:t mahdollistavat tuntemattomien tahojen kryptovaluuttakaupankäynnin esimerkiksi ilman keskitettyjä kolmansia osapuolia. DEX:t jaetaan tyypillisesti kahdenlaiseen luokkaan: tilauskantapohjaiseen DEX:in ja automaattiseen kaupankäyntiin keskittyneisiin älysopimuksiin. Tarjouskirja on perinteiseltä finanssialalta tuttu käsite kaupankäynnistä. Tarjouskirjapohjaisessa kaupankäynnissä kauppa käydään, kun ostaja ja myyjä saavat sovittua yhdessä omaisuuserän, kuten osakkeen, myynnistä ja määrästä. Tällaiset DEX:t ovat jääneet epäsuosioon automaattisten kaupankäyntiin keskittyneiden älysopimusten eli AMM:ien yleistyttyä. AMM-alustat mahdollistavat kryptovaluutanvaihdon automaattisesti hyödyntäen likviditeettipooleja [8]. Näissä likviditeettipooleissa on tyypillisesti kaksi eri valuuttaa, ja pooliin siirtämällä yhtä sen sisältämää valuuttaa, voi vaihtaa itselleen toista poolin valuuttaa [4].

Rug pull -huijausten yleistyminen AMM:issa johtuu siitä, että AMM:ssa kehittäjä voi itse luoda aloituslikviditeetin tokenilleen ja myöskin kontrolloida likviditeettiä itsenäisesti. Koska kehittäjällä on alustavasti valta kontrolloida likviditeettiä, hän voi myös poistaa sen yksipuolisesti. Näin kehittäjä voi tehdä silloin, jos likviditeettiä ei ole lukittu. Likviditeetin poisto on tyypillistä *yksinkertaisessa rug pull* -huijauksessa.

3.4 Rug pull -huijausten taksonomia

Rug pull on yksi kryptovaluuttahuijauksen muoto, jossa huijauksen kohteena ovat tyypillisesti kryptovaluutoista kiinnostuneet sijoittajat. Lisäksi rug pull on DeFi-ekosysteemin yleisin huijausmuoto viime vuosina [2]. Pelkästään vuonna 2021 sijoittajat menettivät 2,8 miljardia Yhdysvaltain dollaria rug pull -huijauksissa [11]. Tämä on Trozze ym. mukaan noin kolmasosa koko DeFi-ekosysteemissä vuonna 2021 huijatusta 7,8 miljardista dollarista. Rug pull -huijauksen perusidea on tapahtuma, jossa kehittäjä tai joukko token-projektin taustalla hylkää projektin ja kavaltaa sijoittajien rahat [8].

Rug pull -huijaukset luokitellaan yleensä kolmeen alalajiin: yksinkertainen (engl. *simple*), uskotteleva (engl. *sell*) ja älysopimustakaovi (engl. *smart contract trap door*) [2, 10, 11]. Sun ym. [12] määrittelee tutkimuksessaan näiden lisäksi kolme lisäkategoriaa, joita ovat likviditeettimanipulaatio (engl. *liquidity pool manipulation*), tokenväärennös (engl. *counterfeit token*) sekä edellä mainittuja luokkia yhdistelevä yhdistelmähuijaus (engl. *combination*).

3.4.1 Yksinkertainen rug pull

Yksinkertainen rug pull on kaikista yleisin ja helpoin tunnistaa rug pull -huijaukseksi. Aluksi DeFi-projektin ja tokenin luonut kehittäjä luo esimerkiksi ERC-20-standardin

mukaisen tokenin. Tämän jälkeen hän luo uuden likviditeettipoolin, jossa hän sitoo tokenin wETH:in tai muuhun tunnettuun tokeniin. Seuraavaksi kehittäjä houkuttelee sijoittajia sijoittamaan projektiin ja tarpeeksi sijoituksia keränneenä lunastaa itselleen kaiken likviditeettipooliin sijoitetun omaisuuden. Likviditeettipoolin tyhjentäminen tällä tavoin edellyttää sitä, että kehittäjä ei ole lukinnut likvideettipoolin likviditeettiä. Tämän taas sijoittaja tunnistaa helposti riskitekijäksi, koska tunnetuissa DeFi-projekteissa likviditeetti on usein lukittu. [10]

3.4.2 Uskotteleva rug pull

Uskotteleva rug pull on perusidealtaan sama kuin yksinkertainen rug pull, mutta sijoittajia pyritään vakuuttamaan valheellisella turvallisuuden tunteella [12]. Tämä turvallisuuden tunne synnytetään sillä, että tokenin likviditeetti on lukittu, eikä kehittäjä voi poistaa sitä.

Kehittäjä ei siis voi yksinkertaisen rug pull -huijauksen tavoin poistaa likviditeettiä ja siten siirtää likviditeettipoolin varoja itselleen samalla tavalla. Sen sijaan joko kehittäjä omistaa alusta alkaen ison määrän huijaustokenia tai hankkii sitä itselleen myöhemmin tavalla tai toisella [2]. Kun huijaustokenin arvo on noussut suhteessa tunnettuun ja arvokkaaseen tokeniin, kuten wETH-tokeniin, hän vaihtaa likviditeettipoolissaan ison määrän huijaustokeniaan tunnettuun tokeniin [11]. Likviditeettipooliin jää iso määrä huijaustokenia ja vain hyvin pieni määrä tunnettua tokenia, jolloin huijaustokenin arvo romahtaa.

3.4.3 Älysopimustakaovi rug pull

Näistä kolmesta rug pull -huijauksen alalajista tunnistettavuudeltaan vaikein on *älysopimustakaovi rug pull* [2, 10]. Tässä huijauksessa tokenin älysopimus sisältää haitallisia funktioita, joilla voidaan esimerkiksi mielivaltaisesti luoda tokenia lisää, siirtää sitä ihmiseltä toiselle tai poistaa kyseistä tokenia liikkelle lasketusta määrästä

[2]. Tyypillistä on myös, että näiden huijausälysopimusten haitalliset funktiot ovat määritelty jossain toisessa, erillisessä älysopimuksessa. Tästä syystä tokenin huijauspyrkimystä on vaikeampi tunnistaa [10]. Älysopimustakaovi-huijauksesta esimerkkinä voidaan pitää projekti BNB42:n tapausta. Projektin kehittäjät käyttivät apuna haitallisia erillisiä älysopimuksia, jotka estivät sijoittajia myymästä tokeniaan. Tästä johtuen noin 6000 sijoittajaa hävisi yhteensä 2,78 miljoonaa Yhdysvaltain dollaria [9].

4 Huijausten analysointi

4.1 Analysoinnin moniulotteisuus

Analysointimenetelmiä Ethereum-lohkoketjussa toimiviin tokeneihin on monia. Tässä alaluvussa vertaillaan viimeaikaisessa tieteellisessä kirjallisuudessa esiteltyjä eri rug pull -huijausten analysointityökaluja sekä niiden hyödyntämiä teknologioita huijausten tunnistamisessa.

Koska analysointi keskittyy yleensä johonkin tiettyyn osa-alueeseen huijauksissa, on tässä luvussa rug pull -huijausten tarkastelu jaettu kolmeen eri ulottuvuuteen: tekniseen, taloudelliseen ja sosiaaliseen. Ensimmäinen eli tekninen ulottuvuus käsittelee älysopimuksiin kirjoitettuja mekanismeja, kuten piilotettuja haitallisia funktioita. Taloudellinen ulottuvuus keskittyy hinnan muutoksen tarkasteluun, likviditeettiin ja tokenin omistajien epätasapainoon. Sosiaalinen ulottuvuus keskittyy lohkoketjujen ulkopuolelle, kuten käyttäjien manipulointiin ja brändin kopiointiin. Tämä jako kolmeen eri ulottuvuuteen mukailee Mothukuri ym. [13] jakoa DeFi-projektin haitallisuustutkimuksen neljään osa-alueeseen:

1. älysopimuksen haavoittuvuusskannaukseen
2. tokenin transaktioiden poikkeavuusskannaukseen
3. tokenin hinnan analysointiin
4. sosiaalisen median seurantaan

Näistä neljästä Mothukuri ym. esittelemästä osa-alueesta koottiin jaottelu tekniseen, taloudelliseen ja sosiaaliseen osa-alueeseen, joista taloudelliseen ulottuvuuteen yhdistetään kohdat 2 ja 3.

Huijaus voi keskittyä näistä ulottuvuuksista yhteen tai se voi yhdistellä useampaa. Seuraavissa alaluvuissa esitellään menetelmiä, jotka havaitsevat kussakin ulottuvuudessa rug pull -huijauksia.

4.1.1 Tekninen ulottuvuus

Monet tutkimukset ja niissä esitellyt työkalut tunnistavat älysopimuksien sisäänrakennettuja haitallisia funktioita. Lin ym. [8] keskittyy tutkimuksessaan esittelemällään työkalullaan *CRPWarner* havaitsemaan teknisiä rug pull -huijauksia. Tutkimuksessa tunnistetaan kolme haitallista funktiota: *hidden mint function*, *limiting sell order* ja *leaking token*. Lisäksi tutkimuksessa tuodaan ilmi, että nämä funktiot voidaan piilottaa ulkoisiin älysopimuksiin, jota rug pull tokenin älysopimus kutsuu. Teknisellä tasolla *CRPWarner* aluksi purkaa älysopimuksen EVM-tavukoodin ja rakentaa siitä ohjausvuokaavion (engl. *control flow graph*, CFG). Sen jälkeen *CRPWarner* suorittaa Datalog-ohjelmointikielellä toteutetut säännöstöt ohjausvuokaaviota vasten, tunnistaen mahdolliset huijaukset.

Myös Zhou ym. [9] tunnistaa ulkoiset älysopimukset yhdeksi uhkaksi. Zhou ym. [9] käsittelee 201 rug pull -tapausta ja keskittyy tutkimuksessaan ennen kaikkea siirtologiikkaa muuttaviin älysopimuksiin. Tutkimuksessa esitellyn Tokeer-työkalun avulla Zhou ym. tunnistavat seuraavat älysopimuksissa esiintyvät funktiot mahdollisiksi uhkiksi: *Blacklist* (käyttäjiltä evätään siirto-oikeuksia), *ModifyBalance* (kehittäjä voi muuttaa mielivaltaisesti tilien saldoja), *TimeLimit* (siirtoja voidaan estää ajallisesti tietyistä osoitteista) ja *AlienDepend* (ulkoisten älysopimusten käyttö). Näillä toiminnoilla poistetaan sijoittajien mahdollisuudet likvidoida tokeninsa juuri ennen kuin tokenin kehittäjä tyhjentää tokenin likviditeetin. Näitä funktioita Tokeer

tunnistaa kohdistamalla Datalog-ohjelmointikielellä ohjelmoituja tunnistussääntöjä *intermediate representation* (IR) -versioon älysopimuksesta. IR-versiolla tarkoitetaan Solidity-älysopimusohjelmointikielen tavukoodiksi käännettyä ja uudelleenjärjesteltyä versiota älysopimuksesta, joka on yksinkertaisempi Datalog-ohjelmointikielellä tehtävää huijauksen tunnistamisvaihetta varten.

Li ym. [14] keskittyy työssään analysoimaan ERC-20-tokeneita älysopimuksen toimituskoodien (engl. *opcode*) avulla. Toimituskoodit ovat kokoelma matalan tason käskyjä, jotka on käännetty älysopimusten korkean tason ohjelmointikielestä tietokoneelle ymmärrettävämpään muotoon. Älysopimuksella tehty tapahtuma koostuu monesta toimituskoodista muodostaen toimituskoodisekvenssin. Li ym. osoittaa, että vertaamalla tutkittavien älysopimusten transaktioiden synnyttämiä toimituskoodisekvenssejä harmittomiksi todettuihin toimituskoodisekvensseihin voidaan tunnistaa haitallisia älysopimuksia.

4.1.2 Taloudellinen ulottuvuus

Taloudellinen analyysi keskittyy lohkoketjussa tapahtuvaan kaupankäyntiin, likviditeetin muutoksiin, tapahtumien aikaleimoihin ja omistajarakenteisiin. Mazorra ym. [10] tarkastelee työssään omistajarakenteita käyttäen apuna Herfindahl—Hirschman-indeksiä (HHI). HHI on yleinen mittari mittaamaan markkinoiden keskittymistä ja sillä voidaan laskea markkinoiden kilpailun määrää. HHI:n määritelmän mukaisesti indeksin arvo on jokin arvo nollan ja yhden välillä. Mitä enemmän markkina on monopolisoitunut, sitä suurempi HHI-arvo on, eli sitä lähempänä se on lukua yksi. Jos taas puolestaan markkinoilla on paljon kilpailua ja kaikki tahot omistavat markkinasta yhtä suuren osan, HHI-arvo on lähenee nollaa.

Tokenia analysoitaessa voidaan huomata, että jos harvat lompakot omistavat ison osan tokenin liikkelle lasketusta määrästä, on tällöin riski, että nämä tahot myyvät oman osuutensa tokenista ravisuttaen tokenin arvoa. Voidaankin päätellä,

että suuri HHI-arvo onkin yhteydessä rug pull -huijaukseen. Mazorra ym. toteaa työssään, että HHI on altis manipuloinnille, koska huijaava taho voi tehdä mielivaltaisen määrän eri lompakko-osoitteita, joille jakaa tokeneita. Näin ollen sijoittaja saa virheellisen kuvan, että tokenin liikkelle lasketusta määrästä kukaan ei omista suurta osaa, vaikka todellisuudessa montaa lompakkoa kontrolloisi sama taho.

4.1.3 Sosiaalinen ulottuvuus

Sosiaalinen analyysi keskittyy tarkkailemaan tokenin saamaa suosiota sosiaalisessa mediassa, joka on yleinen markkinointikanava uusille tokeneille. Shillaus (engl. shilling) tarkoittaa tarkoituksellista toimintaa, jossa kryptovaluuttaprojektia, kuten DeFi-hanketta, NFT:tä (engl. *non-fungible token*) tai muuta sijoituskohdetta, markkinoidaan julkisesti sijoittajien ostohalukkuuden lisäämiseksi [15]. Aggressiivinen shillaus koetaan usein esimerkkinä rug pull -huijauksen tunnuspiirteensä.

Shillauksen tavoitteena voi olla saada sijoittajat tuntemaan pelkoa mahdollisten voittojen ulkopuolelle jäämisestä, kun kyseinen token lähtee kasvattamaan suosiotaan. Tätä pelkoa kuvaava englanninkielinen termi *fear of missing out* (FOMO), on yleinen psykologinen keino saada sijoittajat sijoittamaan tokeniin [13]. Lisäksi sosiaaliseen ulottuvuuteen voidaan liittää esimerkiksi brändin kopionnin havainnointi, jos tokenin nimi tai projekti muuten muistuttaa paljon jotain tunnettua projektia.

4.2 Yhteenveto analyysimenetelmistä

Aiemmin mainitut rug pull -huijausten tunnistusmenetelmät eivät eroa vain tunnistamiseen käytetyssä tiedossa, vaan myös siinä, missä vaiheessa huijaus on mahdollista tunnistaa. Älysopimuksen tekninen analyysi pyrkii tunnistamaan huijauksen jo ennen kuin sijoittajat ehtivät sijoittaa siihen. Taloudellinen analyysi tarvitsee markkinoiden poikkeavuuden havainnointia varten historiallista dataa. Sosiaalisen

ulottuvuuden menetelmät tukevat analyysia tuomalla esiin täysin lohkoketjun ulkopuolista tietoa. Taulukko 4.1 esittelee tunnistusmenetelmät ja niiden tunnistamat uhkat tiivistetysti.

Taulukko 4.1: Eri analyysitasojen analyysimenetelmät, työkalut ja huijaustavat

Ulottuvuus	Tunnistus-menetelmä	Tutkimus	Havaitut huijaustavat
Tekninen	staattinen analyysi, IR-mallinnus, Datalog-säännöt	Lin ym. [8], Zhou ym. [9]	takaovi älysopimuksessa, piilotettu mint-tapahtuma, myynnin esto, blacklist
Taloudellinen	HHI, osoiteklusterit, ML	Mazorra ym. [10], Nguyen ym. [4], Srifa ym. [16], Xia ym. [17]	likviditeetin poistaminen, epänormaalit siirtotapahtumat, tokenin omistajuuden epätasapaino
Sosiaalinen	Regressiomalli, FinBERT (tekoälymalli)	Mothukuri ym. [13], Trozze ym. [11]	shillaus, huijausyhteisöt

5 Pohdinta ja analyysi

Tässä tutkielmassa lähdeaineistona käytetyssä tieteellisessä kirjallisuudessa esitellyt rug pull -huijaustapaukset sekä niiden analysointimenetelmät luokiteltiin kolmeen ulottuvuuteen: tekniseen, taloudelliseen ja sosiaaliseen. Yleensä rug pull -huijaus sisältää toisistaan irrallisia tunnuspiirteitä, kuten esimerkiksi sosiaalisessa mediassa tapahtuva aggressiivinen markkinointi, haitallinen älysopimus ja kehittäjän omistama suuri osuus rug pull -tokenista.

Teknistä ulottuvuutta tutkivat menetelmät havaitsevat poikkeamat älysopimustasolla, mutta eivät havaitse sosiaalista toimintaa tai markkinarakenteita. Taloudellista ulottuvuutta tutkivat menetelmät havaitsevat omistusrakenteen ja likviditeetin poikkeamat, mutta ovat sokeita piilotetuille teknisille takaporteille. Sosiaalista ulottuvuutta tutkivat menetelmät tunnistavat vain täysin lohkoketjun ulkopuolella olevia asioita, jotka ovat hyviä täydentämään analyysia, mutta eivät voi yksin tunnistaa rug pull -huijausta. Keskeistä on, että yksikään menetelmä ei riitä yksistään tunnistamaan rug pull -huijausta.

Teknistä ulottuvuutta tutkivat työkalut, kuten Tokeer [9] ja CRPWarner [8]. Näitä kahta yhdistää kyky tunnistaa haitallisia funktioita älysopimuksissa. Ne onnistuvat havaitsemaan tehokkaasti piilotettuja tokenin luontimekanismeja ja siirtoa rajoittavia mekanismeja jo ennen kuin tokenilla käydään kauppaa. Täten ne ovat tehokkaita ennaltaehkäiseviä työkaluja ja voivat paljastaa rug pull -huijauksen ennen kuin se aiheuttaa menetyksiä sijoittajille. Tekniseen ulottuvuuteen lukeutuvat

tunnistusmenetelmät ovat hyödyllyisiä vain älysopimustakaovi rug pull -huijauksen tunnistuksessa, koska sellaisenaan yksinkertainen tai uskotteleva rug pull -huijaus ei sisällä älysopimuksen suhteen haitallista koodia. Voi kuitenkin olla, että esimerkiksi uskotteleva rug pull -huijaus tehdään juuri siten, että se sisältää myös haitallista koodia. Näin voisi olla esimerkiksi tapauksessa, jossa kehittäjä piilottaa tokenia generoivan *mint*-funktion älysopimukseen, jotta voisi kesken tokenin elinkaarta luoda itselleen tyhjästä lisää tokenia.

Taloudellista ulottuvuutta tutkivat Mazorra ym. [10], Xia ym. [17] ja Srifa ym. [16] havaitsevat menetelmillään likviditeettiin kohdistuvia epäilyttäviä muutoksia, transaktioklustereita, epänormaaleja kaupankäyntejä ennen varsinaista huijausta ja tokenin omistajuuden keskittymiä. Heidän menetelmänsä muiden taloudellista ulottuvuutta tutkivien menetelmien rinnalla kestävät hyvin koodin obfuskointia eli vaikealukuistamista, koska ne eivät pyri tulkitsemaan itse koodia, vaan todistavat siihen perustuvia tapahtumia lohkoketjussa. Näiden menetelmien rajoitteisiin kuuluvat väärät hälytykset eli niin sanotut false positive -tapaukset, joita myös legitiimit projektit voivat laukaista, sillä ne käyttäytyvät usein poikkeuksellisesti projektin alkuvaiheessa. Lisäksi siinä missä älysopimuksia tutkivat tekniset menetelmät tunnistavat huijauksen ennen vahinkoja, taloudellista ulottuvuutta tutkivat menetelmät tarvitsevat lohkoketjudataa analysointiin ja saattavat tunnistaa huijauksen vasta sen tapahduttua.

Sosiaalisen analyysin tehtävä on arvioida sosiaalisessa mediassa tapahtuvan markkinoinnin haitallisuutta. Esimerkiksi voidaan tunnistaa aggressiivinen markkinointi ja selkeä tokenin *shillaus*. Ongelmana kuitenkin on tätä työtä kirjoitettaessa sosiaalista ulottuvuutta käsittelevän kirjallisuuden niukkuus. Tutkimuskirjallisuuden vähyyttää selittänee sosiaaliseen analyysiin liittyvän automatisoinnin hankaluus ja lukuisien eri verkkosivujen ja tiedonlähteiden olemassaolo. Lisäksi tällainen analyysi on manipuloitavissa virheellisellä datalla ja saattaa luoda herkästi *false positive* -

ilmoituksia täysin legitiimeistä tokeneista, joita myöskin markkinoidaan sosiaalisessa mediassa ja joiden markkinointi voi tokeniin sijoittaneiden *shillauksen* ansioista olla aggressiivistakin. Kuten teknistä ja taloudellista ulottuvuutta tutkivat menetelmät, myöskään sosiaalista ulottuvuutta tutkivien menetelmien ja analysointityökalujen käyttö ei yksistään riitä tunnistamaan rug pull -huijausta, mutta tukee kokonaisvaltaista analyysia tuomalla mahdollisia uhkasignaaleja sosiaalisesta mediasta.

Huomataan, että rug pull -huijaukset havaittaisiin parhaiten yhdistämällä älysopimusanalyysi, markkina-analyysi ja sosiaalisen ympäristön muutosten havainnointi. Mothukuri ym. [13] esittelee tutkimuksessaan DeFi-projektin nimeltä *TrustScore*. Kyseinen projekti tutkii halutun tokenin älysopimuksen koodia, tokenin ympärillä tapahtuvia transaktioita, tokenin hinnan vaihtelua ja sosiaalista mediaa ja uutisia tokenin ympärillä. Näistä edellä mainituista tutkinnan kohteista se pisteyttää tokenin luotettavuuden. Tällainen kokonaisvaltainen tokenin analysointi on ollut ja tulee olemaan tärkeää jatkossakin. Vain siten voidaan havaita yksinkertainen, uskotteleva, sekä älysopimustakaovi rug pull -huijaus tehokkaasti.

6 Yhteenveto

Tutkielmassa tarkasteltiin viimeaikaisten tieteellisten julkaisujen avulla hajautetuissa pörsseissä tapahtuvia rug pull -huijauksia ja näiden huijausten analysointimenetelmiä. Tutkielman toisessa luvussa tarkasteltiin aiheen ymmärtämiseen vaadittavia pohjatietoja kryptovaluutoista, lohkoketjuteknologiasta ja älysopimuksista. Kolmas luku käsitteli DeFi-ekosysteemiä ja sen sisältämiä sovellustyyppejä sekä eritteli rug pull -huijausten alaluokkia. Neljännessä luvussa tarkasteltiin viimeaikaisten tieteellisten julkaisujen esittelemiä menetelmiä analysoida rug pull -huijausta teknisillä, taloudellisilla ja sosiaalisilla osa-alueilla. Viidennessä luvussa pohdittiin esiteltyjen analysointimenetelmien käyttökohteita rug pull -huijausten tunnistuksessa. Lopuksi vastataan tutkimuskysymyksiin sekä tarkastellaan tämän tutkielman heikkouksia ja aiheesta nousevia jatkotutkimusideoita.

Ensimmäinen tutkimuskysymys (TK1) selvittää rug pull -huijauksen tyypillisiä tunnuspiirteitä. Teknisesti katsottuna älysopimus voi sisältää haitallisia takaportteja, piilotettuja mint-funktioita, myynnin estäviä funktioita sekä blacklist-funktioita. Taloudellisesta näkökulmasta rug pull -huijaukseen liittyy likviditeetin äkillinen poisto, keskitetty tokenin omistus ja epätavalliset siirtotapahtumat. Sosiaalisesta näkökulmasta rug pull -huijauksen tunnuspiirteet liittyvät aggressiiviiseen shillaukseen, brändin kopiointiin ja huijausyhteisöihin.

Toinen tutkimuskysymys (TK2) selvittää menetelmiä rug pull -huijauksien tunnistukseen. Teknisellä tasolla tehokkaita tunnistusmenetelmiä ovat älysopimuksen

koodin sekä sen suorituksenaikainen analysointi. Näitä voidaan tutkia muuntamalla EVM-tavukoodi CFG- tai IR-malliin ja suorittamalla Datalog-sääntöjä mallia vasten. Epätasapainoisen omistajuuden selvittämiseen sopii Herfindahl–Hirschman-indeksi. Lisäksi osoiteklusteroinnilla voidaan selvittää epätasapainoista omistajuutta tai epätavallisia transaktioita. Sosiaalisella tasolla hyvä tapa olisi verrata tutkittavan tokenin nimeä ja brändiä aiempiin tokeneihin selvittäen mahdollisia brändin kopiointeja. Sosiaalisen median alustoilla ja pikaviestipalveluissa DeFi-projektiin liittyvien julkaistujen tietojen ja mahdollisten *shillaus*-pyrkimysten huomaaminen on huijauksen tunnistuksen kannalta tärkeää.

Vaikkakin tutkielma vastaa sille asetettuihin tutkimuskysymyksiin, on tärkeää huomata, että tutkimuskysymyksiin vastattiin vain käsiteltyjen tieteellisten julkaisujen perusteella. On olemassa yrityksiä, jotka tarjoavat kryptovaluutta-analyysia ja näillä yrityksillä on mahdollisesti omia kehittyneitä työkaluja rug pull -huijausten analysointiin. Lisäksi vapaasti saatavilla olevat avoimen lähdekoodin ohjelmistot saattavat sisältää ajantasaisempia rug pull -huijausten tunnistustyökaluja, joista voitaisiin irrottaa työkalun sisällä toimivat tunnistusmenetelmät. Tutkimuskysymyksiin vastattiin myös hyvin kvalitatiivisesta näkökulmasta ja esimerkiksi tunnistusmenetelmien tehokkuuden mittaus jätettiin huomiotta. Tämä tutkimus sopii luettavaksi kryptovaluutoista ja DeFi-ekosysteemistä kiinnostuneille ja tarjoaa yleiskuvan rug pull -huijauksista.

Monesti rug pull -huijauksia lähestytään usein tietystä, suppeasta näkökulmasta, kuten teknisestä tai sosiaalisesta näkökulmasta. Tämä huomattiin myös tieteellisen kirjallisuuden julkaisuissa. Suppeiden lähestysmitapojen takia joudutaan yhdistelemään eri analyysimenetelmiä ja -työkaluja, jotta rug pull -huijauksia voidaan kokonaisvaltaisesti havainnoida. Jatkotutkimusaiheena kirjallisuudessa esitellyistä tunnistusmenetelmistä voitaisiin koostaa kokonaisvaltaisia tunnistustyökaluja. Jatkotutkimuksena voitaisiin myös pohtia tapoja, joilla sijoittajat voisivat helposti tun-

nistaa rug pull -huijauksia tai miten hajautettujen pörssien olisi otettava vastuuta rug pull -huijauksien ehkäisyssä.

Lähdeluettelo

[1] C. Wu et al., "Profit or Deceit? Mitigating Pump and Dump in DeFi via Graph and Contrastive Learning", *IEEE Transactions on Information Forensics and Security*, vol. 20, s. 8994–9008, 2025, ISSN: 1556-6021. DOI: 10.1109/TIFS.2025.3594873.

[2] C. Sechting ja P. Raschke, "A Taxonomy of Anti-Fraud Measures within Token Economy: Insights from Rug Pull Schemes", teoksessa *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Berlin, Germany, lokakuu 2024, s. 1–9. DOI: 10.1109/BRAINS63024.2024.10732222.

[3] P. Qian et al., "Comprehensive review of smart contract and DeFi security: Attack, vulnerability detection, and automated repair", *Expert Systems with Applications*, vol. 291, s. 128 431, lokakuu 2025, ISSN: 0957-4174. DOI: 10.1016/j.eswa.2025.128431.

[4] M. H. Nguyen, P. D. Huynh, S. H. Dau ja X. Li, "Rug-pull malicious token detection on blockchain using supervised learning with feature engineering", teoksessa *Proceedings of the 2023 Australasian Computer Science Week*, sarja ACSW '23, New York, NY, USA: Association for Computing Machinery, 2023, s. 72–81, ISBN: 979-8-4007-0005-7. DOI: 10.1145/3579375.3579385.

[5] S. Zhang, C. Hu, T. Lan, L. Wang, S. Xu ja W. Shao, "Intelligent Contract Vulnerability Detection Method Based on Bic-RL", teoksessa *2023 Interna-*

tional Conference on Data Security and Privacy Protection (DSPP), Xi'an, China, lokakuu 2023, s. 128–135. DOI: 10.1109/DSPP58763.2023.10404628.

[6] V. Buterin, *Ethereum Whitepaper*. viitattu 7. tammikuuta 2026. url: https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.

[7] Y. Xue et al., "A Review on the Security of the Ethereum-Based DeFi Ecosystem", en, *Computer Modeling in Engineering & Sciences*, vol. 139, nro 1, s. 69–101, 2023, ISSN: 1526-1492, 1526-1506. DOI: 10.32604/cmes.2023.031488.

[8] Z. Lin, J. Chen, J. Wu, W. Zhang, Y. Wang ja Z. Zheng, "CRPWarner: Warning the Risk of Contract-Related Rug Pull in DeFi Smart Contracts", *IEEE Transactions on Software Engineering*, vol. 50, nro 6, s. 1534–1547, kesäkuu 2024, ISSN: 1939-3520. DOI: 10.1109/TSE.2024.3392451.

[9] Y. Zhou, J. Sun, F. Ma, Y. Chen, Z. Yan ja Y. Jiang, "Stop Pulling my Rug: Exposing Rug Pull Risks in Crypto Token to Investors", teoksessa *2024 IEEE/ACM 46th International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, Lisbon, Portugal, huhtikuu 2024, s. 228–239. DOI: 10.1145/3639477.3639722.

[10] B. Mazorra, V. Adan ja V. Daza, "Do Not Rug on Me: Leveraging Machine Learning Techniques for Automated Scam Detection", *Mathematics*, vol. 10, nro 6, s. 949, maaliskuu 2022, ISSN: 2227-7390. DOI: 10.3390/math10060949.

[11] A. Trozze, T. Davies ja B. Kleinberg, "Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering", *Forensic Science International: Digital Investigation*, vol. 46, s. 301 575, syyskuu 2023, ISSN: 2666-2817. DOI: 10.1016/j.fsidi.2023.301575.

[12] D. Sun, W. Ma, L. Nie ja Y. Liu, ”SoK: A Taxonomic Analysis of DeFi Rug Pulls: Types, Dataset, and Tool Assessment”, *Proceedings of the ACM on Software Engineering*, vol. 2, nro ISSTA, ISSTA025:550–ISSTA025:572, 2025. DOI: 10.1145/3728900.

[13] V. Mothukuri, R. M. Parizi, J. L. Massa ja A. Yazdinejad, ”An AI Multi-Model Approach to DeFi Project Trust Scoring and Security”, teoksessa *2024 IEEE International Conference on Blockchain (Blockchain)*, Copenhagen, Denmark, elokuu 2024, s. 19–28. DOI: 10.1109/Blockchain62396.2024.00013.

[14] P. Li, G. Wang, X. Xing, J. Zhu, W. Gu ja G. Zhai, ”Detecting abnormal behaviors in smart contracts using opcode sequences”, *Computer Communications*, vol. 220, s. 12–22, huhtikuu 2024, ISSN: 0140-3664. DOI: 10.1016/j.comcom.2024.03.016.

[15] Coinmotion team, *Mitä kryptotermit tarkoittavat? – osa 2*, marraskuu 2024. viitattu 7. joulukuuta 2025. url: https://coinmotion.com/fi/mita-kryptotermit-tarkoittavat-osa-2/.

[16] S. Srifa, Y. Yanovich, R. Vasilyev, T. Rupasinghe ja V. Amelin, ”Rug pull detection on decentralized exchange using transaction data”, *Blockchain: Research and Applications*, vol. 6, nro 3, s. 100 275, syyskuu 2025, ISSN: 2096-7209. DOI: 10.1016/j.bcra.2025.100275.

[17] P. Xia et al., ”Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange”, teoksessa *Abstract Proceedings of the 2022 ACM SIGMETRICS/IFIP PERFORMANCE Joint International Conference on Measurement and Modeling of Computer Systems*, sarja SIGMETRICS/PERFORMANCE ’22, New York, NY, USA: Association for Computing Machinery, 2022, s. 23–24, ISBN: 978-1-4503-9141-2. DOI: 10.1145/3489048.3522636.