Am I Here For The Tech? — L1-lohkoketjujen ominaisuuksien arvostus

Diplomityö
Turun yliopisto
Tietotekniikan laitos
Ohjelmistotekniikka
2022
Arttu Laitinen

TURUN YLIOPISTO
Tietotekniikan laitos

Arttu Laitinen: Am I Here For The Tech? — L1-lohkoketjujen ominaisuuksien arvostus

Diplomityö, 70 s.
Ohjelmistotekniikka
Joulukuu 2022

2010-luvun aikana lohkoketjuteknologia ja kryptovaluutat muodostivat uuden talouden ja teknologian sektorin, jonka vaikutusten ennakointi oli mahdotonta. Anonyymin nimimerkin takaa kirjoitettu Bitcoinin toimintaperiaatteen selittävä julkaisu aloitti liikkeen, joka kasvoi alle kymmenessä vuodessa teknologiaharrastajien spekulaatioista parhaimmillaan yli kolmen biljoonan dollarin toimialaksi. Miten tätä nopeasti kehittyvää kokonaisuutta tulisi edes yrittää ymmärtää?

Tämä tutkimus tarkastelee lohkoketjualaa tutkimalla *ensimmäisen asteen lohkoketjujen* (eng. layer 1, L1) ominaisuuksia. Tutkimuksessa avataan eri lohkoketjuteknologiaan liittyviä konsepteja sekä syvennytään kyselytutkimuksen avulla määrittelemään ominaisuuksien välisiä painoarvoja. Tutkimus selvittää mille asioille alalla toimivat antavat arvoa ja pyrkii osaltaan helpottamaan lohkoketjujen konseptilabyrintissa navigointia.

Tutkimus on toteutettu kyselytutkimuksena, johon on haastateltu 33 lohkoketjuteknologian ja kryptovaluuttojen parissa toimivaa henkilöä. Tutkimuksen avulla lohkoketjujen ominaisuuksille voitiin määrittää suhteellinen painokerroin, joka kuvaa ominaisuudelle annettua painoarvoa. Kyselyä taustoittavan kirjallisen osion lähdemateriaalina on käytetty laajasti kryptoalasta tuotettua tieteellistä ja ei-tieteellistä kirjallista aineistoa, jota hyödyntäen kuvataan lohkoketjuteknologian olennisimmat rakenneosat. Tilastotietoa on kerätty myös erilaisista lohkoketjuja ja kryptovaluuttoja analysoivista palveluista.

Asiasanat: Lohkoketjuteknologia, L1-lohkoketju, kryptovaluutta

Sisällys

Kuvat

Taulukot

1 Johdanto

1.1 Tutkimuksen teon taustamotiivit: Paradigmamuutos

Talousjärjestelmällä voidaan sanoa olevan kuusi perusfunktiota; maksujen välittäminen, resurssien kokoaminen ja osuuksien jakaminen, resurssien siirto ajan ja sijainnin suhteen, riskinhallinta, informaation välitys ja kannustinongelmin hallinta [1]. On kyseessä sitten Venetsialainen pankki 1100-luvulla tai nykyisin toimiva New Yorkin pörssi, ovat finanssi-instituutiot muodostuneet tarjoamaan palveluita ja toimimaan luotettuina välimiehinä näiden perusfunktioiden ympärille. Ilman pankkien, keskitettyjen kauppapaikkojen tai vakuutusyhtiöiden toimintaa olisi vaihdanta merkittävästi vaikeampaa ja kalliimpaa, ellei peräti mahdotonta. Tämä osoittaa kyseisten organisaatioiden tarjoamien palvelujen kiistattoman merkityksen nykyiselle talousjärjestelmälle [2]. Olennaista on kuitenkin havaita, että merkityksellisiä ovat juuri talousjärjestelmän perusfunktiot ja siten organisaatioiden palvelut, eivät vakiintuneet talousorganisaatiot itsessään. Funktiot ovat organisaatioita vakaampia, muuttuvat hitaammin ja ovat samankaltaisia ympäri maailman, vaikka esimerkiksi pankit ovat olleet ja ovat huomattavan erilaisia ajasta ja paikasta riippuen. [1]

Talousteknologialla, (engl. fintech, financial technology) tarkoitetaan hiljattain kehitettyä digitaalista teknologiaa, jota käytetään tai tullaan lähitulevaisuudessa käyttämään finanssipalveluiden tarjoamiseen. Ala on kasvanut merkittävästi viime

vuosikymmenen aikana. Tarjoamalla uudenlaisia digitaalisia talouspalveluja uudet yritykset uhkaavat vakiintuneiden toimijoiden, kuten perinteisten pankkien, toimintaa. Vaikka uudet fintech-yritykset vähentävätkin finanssi-instituutioiden vaikutusvaltaa, eivät ne lähtökohtaisesti poista tarvetta välimiehille. Käytännössä järjestelmä pysyy edelleen keskitettynä, välimiehet vain vaihtuvat. [3]

Historia osoittaa myös nykyisen keskitetyn talousjärjestelmän heikkoudet. Luotetuilla välimiehillä on merkittävä valta vaihdannassa ja tätä valtaa voidaan käyttää vipuvoimana omien taloudellisten intressien tavoittelussa. Yhtenä räikeimmistä esimerkeistä on 2008 Lehmann Brothersin konkurssista alkanut finanssikriisi.

On ilmeistä, että täydellisen tehokkaassa markkinassa, ilman transaktiokuluja, informaatiokuluja tai jakamattomuuksia, ei välimiehiä olisi olemassa [2]. Lohkoketjuteknologia on innovaatio, joka ensimmäistä kertaa mahdollistaa sähköisessä järjestelmässä luotettavan vaihdannan vertaisverkossa ilman erillistä luotettua välimiestä [4]. Käytännössä teknologia mahdollistaa kaikkien talousjärjestelmän perusfunktioiden erottamisen perinteisitä finanssitoimijoista ja samojen toiminnallisuuksien ja palvelujen tarjoamisen hajautetusti, teknologialähtöisesti ja ilman keskitettyä valtaa järjestelmään.

Kyseinen arvolupaus on vuoteen 2021 mennessä kasvattanut lohkoketjuteknologian ympärille usean biljoonan euron arvoisen ja valtavan nopeasti kehittyvän teknologia-alan. Periaatteet hajautuksen ympärillä ovat myös mahdollistaneet valtavan käyttöönoton lisääntymisen ruohonjuuritasolta lähtien ja yksilöt ja organisaatiot ovat voineet sijoittaa rahojaan monimuotoisiin kryptovaluuttoihin ja projekteihin. Alalla on nähty satumaisia arvonnousuja ja rikastumisia, mikä on entisestään lietsonut huumaa ja kiinnostusta. Samaan aikaan alan sääntely, kuten muillakin nopeasti kehittyvillä ja innovatiivisilla teknologia-aloilla, on jäänyt jälkeen ja esimerkiksi huijauksilta ei olla voitu välttyä. Moni pitää kryptoalaa edelleen vain hollantilaisen tulppaanikuplan ilmentymänä.

Lohkoketjuteknologiaan ja kryptosektoriin liittyy paljon kiinnostusta, mutta myös paljon teknistä ja taloudellista kompleksisuutta. Alalla tehdään jatkuvasti uusia innovaatioita ja teknologia kehittyy valtavasti, mikä houkuttelee uusia ihmisiä lohkoketjuteknologian pariin. Yleinen uskomus onkin, että merkittävä osa lohkoketjun ja kryptovaluuttojen pariin päätyvistä ihmisistä eivät ymmärrä taustalla vaikuttavaa teknologiaa alkuunkaan. "I am here for the tech"on yleinen, jopa vitsiksi ja meemiksi kääntynyt kommentti, jota viljellään eri teknolgia- ja sijoitusfoorumeilla, kun monimutkaiset konseptit menevät yli hilseen. Ovatko alaan resurssejaan investoimassa aidosti rakentamassa web 3.0-vallankumousta, vai mukana vain ollakseen osana kurssinousujen siivittämää uhkapelihurmosta?

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tämän tutkimuksen tavoitteena on selvittää mitä lohkoketjuekosysteeminen ominaisuuksia lohkoketjuteknologian parissa toimivat ja kryptovaluuttoihin sijoittaneet yksilöt pitävät tärkeinä. Tutkimuksen päätutkimuskysymykseksi muodostuu:

TK1: *Mitkä ensimmäisen asteen lohkoketjun ominaisuudet ovat tärkeimpiä?*

Tutkimuksessa pyritään selvittämään eroavatko lohkoketjuteknologiaan ensisijaisesti sijoittavien ihmisten arvostuksen kohteet (sijoittajanäkökulma) lohkoketjuteknologian kehityksen parissa toimivien ihmisten arvostamista ominaisuuksista (kehittäjänäkökulma). Tutkimukselle muodostuu jatkotutkimuskysymys:

TK2: *Miten sijoittajanäkökulma eroaa kehittäjänäkökulmasta ominaisuuksia arvottaessa?*

Tutkimuksessa pyritään myös selvittämään mikäli lohkoketjuteknologian parissa vietetty aika vaikuttaa arvostuksen kohteisiin, josta muodostuu kolmas ja neljäs jatkotutkimuskysymys:

TK3: *Onko kokemusvuosilla vaikutusta ominaisuuksien arvotukseen?*

TK4: *Onko suuremalla aktiivisuudella lohkoketju- ja virtuaalivaluuttateemojen*

parissa vaikutusta ominaisuuksien arvostukseen?

Vaikka tutkimuksessa vertaillaan eri lohkoketjuja ja esimerkinomaisesti niiden teknisiäkin elementtejä, on ensisijainen tarkoitus tutkia ihmisten suhtautumista näihin elementteihin. Tarkoitus ei ole erityisesti vertailla eri lohkoketjujen paremmuutta, vaan korostaa niiden eroja.

Lohkoketju on suhteellisen uusi, hyvin monimutkainen ja kerrostunut teknologiakonsepti. Tämän tutkimuksen laajuus on rajattu erityisesti nk. *ensimmäisen asteen lohkoketjuihin* (engl. layer 1, L1). Tutkimuksen ulkopuolelle jätetään esimerkiksi eri lohkoketjujen päälle rakennettujen *hajautetuille sovelluksille* (engl. decentralized application, dapp) sekä *toisen asteen* (engl. layer 2, L2) skaalautumisratkaisuille ominaisten elementtien tarkastelu.

1.3 Tutkimusmenetelmä ja tutkimusaineisto

Tämä tutkimus toteutetaan kvantitatiivisena eli määrällisenä tutkimuksena. Tutkimusaineisto kerätään kyselytutkimuksen avulla. Kysely on toteutettu verkossa ja siihen on pyritty vastaajiksi tavoittamaan lohkoketjuteknologioiden parissa toimineita ja kryptovaluuttoihin sijoittaneita yksilöitä. Kyselyä on jaettu avoimesti kirjoittajan LinkedIn- ja Twitter-profiilien päivityksissä, työyhteisön Slack-kanavalla sekä kolmen eri lohkoketjuprotokollan kehitys- ja käyttäjäyhteisön discord-kanavilla. Kyselyn kysymykset on luotu pohjautuen aiempaan teoriatietoon ensimmäisen asteen lohkoketjuista. Kyselylomakkeen tuloksia muokataan paremmin luettavaan taulukkomuotoon ja niitä analysoidaan regressioanalyysin ja yhteisvaihtelun analyysin avulla.

1.4 Tutkimuksen rakenne

Tässä tutkimuksessa käsitellään lohkoketjuteknologiaa, sekä sen varaan rakennettuja eri lohkoketjuekosysteemejä ja niiden ominaisuuksia. Tutkimuksen tarkoituksena on selvittää, mitä kyseisestä teknologia-alasta kiinnostuneet ja siihen investoineet ihmiset pitävät tärkeinä lohkoketjujen ominaisuuksina. Tutkimus keskittyy analysoimaan erityisesti *ensimmäisen asteen lohkoketjuja* (engl. layer 1, L1).

Tutkimus koostuu kahdesta osiosta: teoriaosuudesta ja tutkimusosuudesta, jotka on jaettu yhteensä viiteen päälukuun.

Ensimmäisessä luvussa, eli johdannossa, kerrotaan lyhyesti motiivi tutkimuksen taustalla, käydään läpi tutkimuksen tavoitteet ja tutkimuskysymykset sekä tutkimusmenetelmä ja käytetty tutkimusaineisto ja kuvataan tutkimuksen kokonaisrakenne.

Toisessa luvussa käsitellään kirjallisuuskatsauksen keinoin tutkimuksen taustateoriaa eli lohkoketjuteknologian kehitystä kronologisessa järjestyksessä. Luvun tarkoituksena selventää lohkoketjuihin liittyviä peruskäsitteitä ja -konsepteja, joiden ymmärtäminen on oleellista lohkoketjuekosysteemien myöhempään tarkasteluun. Luku on jaettu kolmeen kappaleeseen, jotka kuvaavat lohkoketjuteknologian kehityksen eri sukupolvia. Kappaleissa avataan kunkin kauden olennaisia innovaatioita ja käsitteitä.

Kolmannessa luvussa jatketaan edelleen taustateorian parissa. Siinä tarkastellaan tarkemmin moderneille L1-lohkoketjuille olennaisia ominaisuuksia, joiden avulla eri L1-lohkoketjujen välisiä eroja voidaan havainnollistaa ja joiden avulla niitä on mielekästä vertailla. Luvussa myös tarkastellaan lohkoketjujen ominaisuuksien vertailuun liittyviä aikaisempia tutkimuksia.

Neljännessä luvussa kuvataan tarkemmin toteutettu määrällinen kyselytutkimus. Siinä tarkastellaan tutkimusmenetelmää ja tutkimusaineistoa.

Viidennessä luvussa tutkimuksen tulokset kootaan yhteen johtopäätöksiä varten.

Luvussa myös käsitellään sopivia aiheita jatkotutkimuksen aiheiksi.

2 Lohkoketjuteknologia

Tutkimuksen tarkoituksena on tarkastella mitä lohkoketjuekosysteemien ominaisuuksia teknologian parissa toimivat ja kryptovaluuttoihin sijoittaneet yksilöt pitävät tärkeinä. Lohkoketju on verrattain uusi ja monitahoinen teknologia, jonka eri ominaisuuksien keskinäisten suhteiden ja merkityksen ymmärtämistä helpottaa merkittävästi sen tärkeimpien kehitysvaiheiden tunteminen. Siksi tässä luvussa käsitellään lohkoketjuteknologian kehitystä kronologisesti vuodesta 2008 vuoteen 2022.

Lohkoketjujen kehitysvaiheet voidaan karkeasti jakaa kolmeen sukupolveen. Ensimmäisen lohkoketjusukupolven aloitti Bitcoin, joka oli ensimmäinen toimiva sovellus hajautetusta digitaalisesta maksujärjestelmästä. Bitcoin osoitti, että hajautetuilla teknologioilla voidaan toteuttaa luotettavasti toimiva valuuttajärjestelmä ilman, että järjestelmän yksittäisiin toimijoihin luotetaan [4]. Ethereum synnytti toisen sukupolven tuoden mukanaan älysopimukset, jotka mahdollistivat monipuolisten sovellusten rakentamisen hajautetusti [5]. Kolmannen sukupolven lohkoketjuja ovat vuoden 2017 jälkeen kehitettyjä ns. ethereumintappajia, jotka ovat joukko jatkuvasti nopeammin kehittyviä uusia lohkoketjuverkostoja ja joiden ensisijainen tarkoitus on syrjäyttää Ethereum vakiintuneena hajautettuna sovellusalustana. Tässä luvussa tarkastelu painottuu erityisesti kahteen ensimmäiseen sukupolveen, sillä ne ovat luoneet perustan merkittävälle osalle lohkoketjujen eri konsepteista. Kolmatta sukupolvea tarkastellaan välillisesti kolmannessa luvussa, kun perehdytään tarkemmin L1-lohkoketjujen ominaisuuksiin. [6]

2.1 Ensimmäinen sukupolvi: Bitcoin

Tässä kappaleessa tarkastellaan Bitcoinin innovatiivisia elementtejä ja toimintaperiaatetta. Bitcoin-verkon ollessa ensimmäinen lohkoketjuteknologian varaan rakennettu sovellus, eli ensimmäinen lohkoketjuverkko, voidaan sitä yleisesti pitää eräänlaisena lohkoketjuteknologian perustapauksena, johon myöhempiä kehitysvaiheita on suoraviivaista verrata.

2.1.1 Bitcoin innovaationa

31.10.2008 pseudonyymi Satoshi Nakamoto julkaisi artikkelin, joka kuvasi uudenlaisen sähköisen valuuttajärjestelmän toimintaperiaatteen [7]. Kyseessä oli Bitcoin - täysin vertaisverkossa toimiva sähköinen maksujärjestelmä. Merkittäväksi Bitcoinin teki sen ratkaisu klassiseen Bysantin kenraalin ongelmaan. Se ei toimiakseen vaatinut keskitettyä ja luotettua osapuolta, kuten pankkia tai muuta maksunvälittäjää, vaan kaikki osapuolet saivat pitää anonymiteettinsä. [4]

Bysantin kenraalin ongelmalla tarkoitetaan tilannetta, jossa hypoteettisesti kaupunkia piirittävien kenraalien tulisi sopia hyökkäyssuunnitelmasta kommunikoiden vain yhdensuuntaisin viestein. Ongelman muodostaa se, että yksi tai useampi kenraaleista saattaa olla petturi. Tietokonejärjestelmissä tällä voidaan tarkoittaa tilannetta, jossa järjestelmän eri osat virhetilanteessa lähettävät keskenään ristiriitaisia viestejä. Sekä Bysantin kenraaleilla että luotettavilla tietokonejärjestelmillä tulisi olla menetelmä, jolla käsitellä ongelmaa. Tällöin puhutaan *Bysantin vikasietoisesta järjestelmästä* (engl. byzantine fault tolerance, BFT). [8]

Bysantin kenraalien ongelman yksi olennainen sovellutus maksujärjestelmissä on *kaksoiskulutus*. Kaksoiskulutuksella (engl. double spending) tarkoitetaan tilannetta, jossa järjestelmä mahdollistaa saman krediitin maksamisen vilpillisesti samanaikaisesti usealle eri vastaanottajalle. Tällöin maksaja todellisuudessa käyttää maksamiseen krediittejä, jotka hän on jo kerran käyttänyt ja joita hänellä ei oikeasti olisi

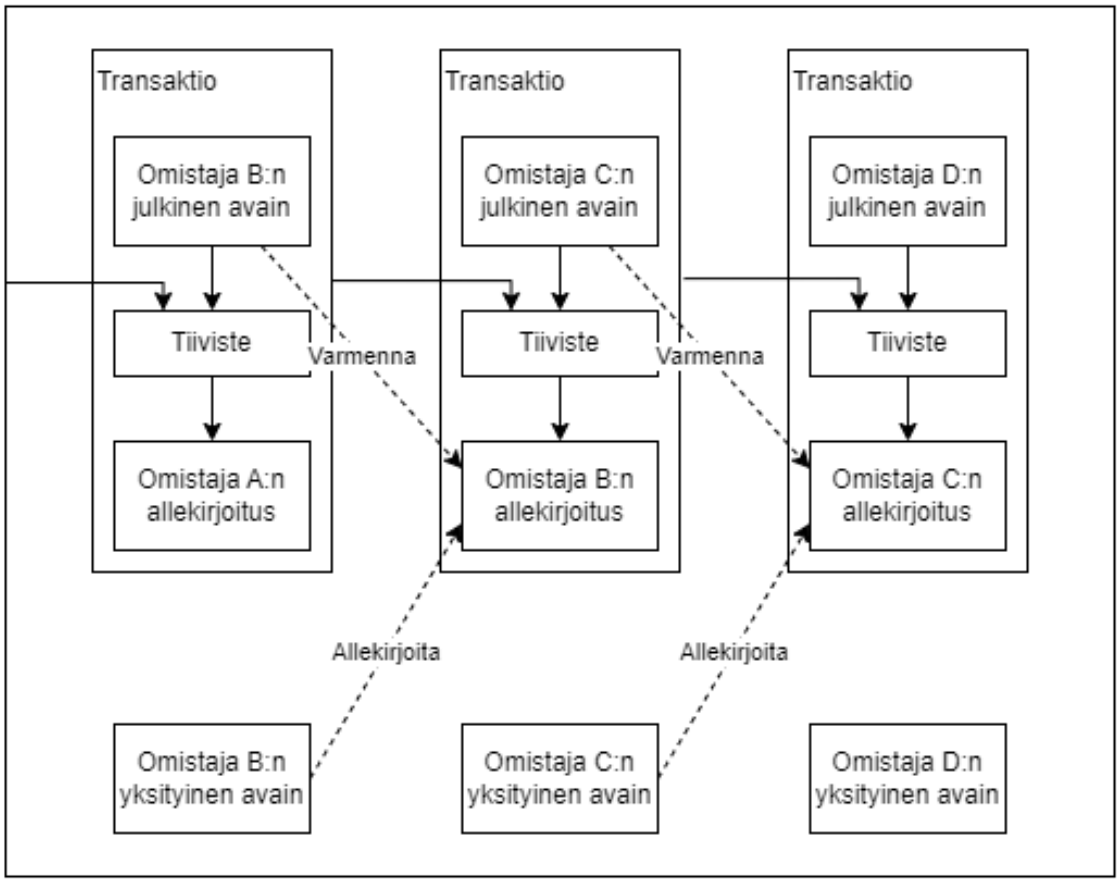
käytettävänään. Bitcoinin luomiseen asti välimiehetön toiminta oli ollut mahdollista vain fyysisen valuutan avulla, muttei sähköisissä palveluissa. Bitcoin ei ollut ensimmäinen yritys toteuttaa virtuaalivaluuttaa ja sitä oli edeltänyt mm. Wei Dain kehittämä b-money vuodelta 1998 [9]. Nakamoton kehittämä lohkoketju oli kuitenkin ensimmäinen kokonaisuus, jossa ei asetettu vaatimuksia järjestelmän osien luotettavuudelle. Bitcoin oli rakennettu toimimaan kokonaan *luottamattomana* (engl. trustless) ja oli Bysantin vikasietoinen myös anonyymien ja siten epäluotettavien käyttäjien käyttämänä. [4]

2.1.2 Bitcoinin toimintaperiaate

Bitcoinin toiminnan pohjana olevan lohkoketjun muodostaa ketjutettu listaus tilitapahtumia, jotka kirjataan hajautettuun, avoimeen ja muuttumattomaan tilikirjaan. Lohkoketjuteknologiaan viitataan usein juuri *hajautettuna tilikirjana* (engl. distributed ledger). Bitcoin-verkon muodostavat kahdenlaiset *noodit* (engl. node), joilla tarkoitetaan toisiinsa esimerkiksi internetin avulla yhteenkytkettyjä tietokoneita. *Varmentajat* (engl. validator) vahvistavat tehtyjen transaktioiden oikeellisuuden ja ylläpitävät Bitcoinin transaktiohistoriaa. Käytännössä kuka vain voi alkaa noodin ylläpitäjäksi ja varmentajaksi. Varmentajat ovat keskeisessä asemassa verkon turvallisuuden ylläpitämisessä, sillä mitä enemmän varmentajia tarkastelee transaktioita, sitä pienemmäksi käy todennäköisyys vilpillisten transaktioiden huomioimattomuudesta. Yksinkertaisimillaan varmentajat varmistavat, että tarjolla on oikeasti tarpeeksi valuuttaa aiottujen maksujen suorittamiseen. [4]

Kun taho A haluaa välittää taholle B bitcoin-valuuttaa, hän ilmoittaa Bitcoin verkolle transaktiosta. Käytännössä ilmoitus pitää sisällään viitteen aiempiin transaktioihin, tehtävän maksun kohdeosoitteen ja siirrettävän valuuttamäärän. Koska maksuja ei hallinnoi välimies, vaan ne hoidetaan hajautetusti, on ilmoituksen oltava julkinen [9]. Lohkoketjuteknologia perustuu julkisen avaimen infrastruktuuriin

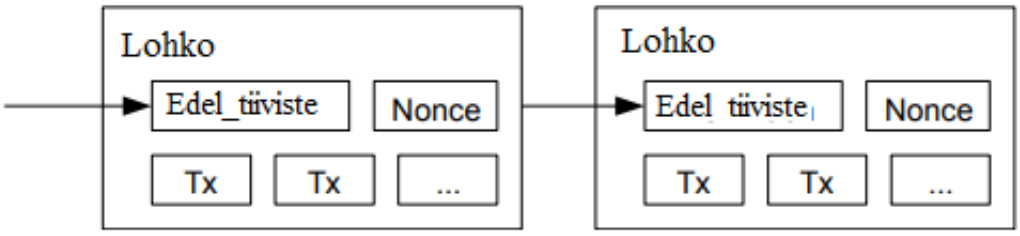
ja transaktiot valtuutetaan käyttäen lähettäjän yksityistä avainta. Transaktioden valtuutus tarkastetaan julkista avainta vasten, jonka jälkeen se välitetään noodien välityksellä ns. *muistialtaaseen* (engl. memory pool tai mempool) odottamaan. Itse maksutapahtuman kirjaamiseksi järjestelmä tarvitsee erikoistuneita noodeja, joita kutsutaan *louhijoiksi* (engl. miner). Louhijoiden tehtävänä on kerätä uudet vielä varmentamattomia transaktioita muistialtaasta yhteen ja muodostaa niistä uusi lohko liitettäväksi lohkoketjun jatkeeksi. Noodien tapaan kuka vain verkon jäsen voi ryhtyä louhijaksi halutessaan. [4]



Kuva 2.1: Havainnekuva Bitcoin-transaktion varmentamisesta [4]

Jotta transaktiot muodostaisivat ehyen maksuhistorian, on ne kirjattava ketjuun oikeassa järjestyksessä. Louhijoiden on voitava määritellä keskenään, kuka muodos-

taa seuraavan lohkon. Tätä päätöksenteon vaihetta kutsutaan konsensusmekanismiksi, joka on lohkoketjun innovaation ydin. Bitcoinin käyttää konsensuksen muodostamiseen *työtodistus*-nimistä (engl.proof of work, PoW) konsensusmekanismia, jossa louhijat etsivät sopivaa kriteerit täyttävää kryptografista SHA-256 *tiivistettä* (engl. hash). SHA-256 on yhdensuuntainen tiivistefunktio, joka tiivistää minkä vain syötteen 256 tavun pituiseksi. SHA-256:ta pidetään kryptografisesti turvallisena [10]. Syötteen osana tiivisteen etsimiseen käytetään edellisen lohkon tunnistetta, joka on myös tiiviste sitä aikaisemman lohkon tunnisteesta. Lisäksi syötteen osana on ns. *kertakäyttöluku* (engl. nonce), mikä selviää vain arvaamalla. Käytännössä louhijat käyttävät prosessorien laskentatehoa laskemaan SHA-256 tiivisteitä eri syötteillä, kunnes joku saa sattumanvaraisesti osuman uuden lohkon tiivisteeksi. Uusia Bitcoin-lohkoja luodaan keskimäärin 10 minuutin välein. Protokolla ylläpitää tätä lohkoaikaa muuttamalla dynaamisesti seuraavan lohkon tiivisteen kriteerejä ja siten löytämisen vaikeusastetta sen mukaan, miten paljon laskentatehoa verkossa käytetään louhimiseen. [4]



Kuva 2.2: Havainnekuva Bitcoin-lohkon koostumuksesta [4]

Kun sopiva tiiviste löytyy, muodostuu uusi lohko, johon louhija kerää muistialtaasta transaktioita. Transaktioiden määrää rajoittaa lohkon tallennuskapasiteetti eli ns. *lohkokoko* (engl. block-size), joka Bitcoin-lohkoketjussa on kirjoittamishetkellä noin 1MB. Uuden lohkon (n) löytyessä ja noodien varmentaessa lohkon osaksi

ketjua, siirtyvät louhijat louhimaan uutta tiivistettä lohkolle (n+1). [4]

Bitcoinin tapauksessa uusia lohkoja syntyy keskimäärin 10 minuutin välein, mutta on mahdollista, että lohkoja löytyy useampia jopa samaan aikaan. Tällöin ketju *haarautuu* (engl. fork). Tämä luonnollisesti aiheuttaa intressiristiriidan eri haarojen muodostamien eri totuuksien välillä ja ajoittain on mahdollista, että merkittävä osa louhintatehosta on hajautunut useampaan eri haaraan. Käytännössä kuitenkin pääosa louhijoista siirtyy hyvin nopeasti edistämään pisintä haaraa, kun eroa muodostuu ja kilpailun hävinneet haarat jäävät merkitysettömiksi. [4]

Louhintaprosessi kuluttaa paljon laskentatehoa, joten järjestelmään on kehitetty insentivointimenetelmä kannustamaan uusien lohkojen etsimistä. Kun uusi lohko löytyy, maksetaan louhijalle louhintapalkkio. Louhintapalkkio oli aluksi 50 bitcoinia, mutta määrä puolittuu aina 210 000 lohkon välein. Huomioiden Bitcoin-verkon 10 minuutin lohkoajan, tapahtuu palkkion *puoliintuminen* (engl. halving) noin neljän vuoden välein. Louhintapalkkion lisäksi louhijat saavat kustakin kirjaamastaan transaktiosta välityspalkkion. Yksittäinen bitcoin-rahakkeiden louhija voi parantaa omia mahdollisuuksiaan löytää sopiva tiivistefunktio ennen muita käyttämällä suuremman määrän laskentatehoa ja siten lisäämällä frekvenssiä, jolla arvaa uusia tiivistefunktion syötteitä. Louhijan *tiivistefrekvenssin* (engl. hashrate) on kasvettava suhteessa Koko Bitcoin-verkon tiivistefrekvenssiin lohkon löytämisen todennäköisyyden kasvattamiseksi. [4]

Louhijoiden määrä ja siten protokollan tiivistefrekvenssi ovat merkittäviä Bitcoin-protokollan turvallisuuteen vaikuttavia tekijöitä. Vilpillinen taho tai vilpillisten tahojen yhteenliittymä voi hallitsemalla enemmistöä verkon tiivistefrekvenssistä sisällyttää lohkoihin vilpillisiä ja virheellisiä transaktioita. Käytännössä vilpilliset tahot varmistavat, että korruptoitunut haara pitenee nopeimmin, jolloin myös rehelliset toimijat päätyvät sen ennen pitkään hyväksymään. Tätä menetelmää kutsutaan 51% hyökkäykseksi. Kyseistä hyökkäystä vastaan verkko on suojassa parhaiten, kun sen

tiivistefrekvenssi on suuri ja enemmistön laskentatehosta haaliminen vilpillisille toimijoille on kestämättömän kallista [11]. On myös ilmeistä, että mitä suuremmalle joukolle louhijoita laskentateho tiivistefrekvenssi hajautuu, sitä vaikeampaa on luoda vilpillisiä yhteenliittymiä enemmistön saavuttamiseksi. [4]

Koska lohkoketjuprotokollat ovat hajautettuja, niiden päivittäminen ei ole suoraviivaista. Käytännössä verkon ohjelmisto päivittyy, mikäli verkon noodit ottavat uuden ohjelmistoversion käyttöön. Uudet ohjelmistoversiot käytännössä muodostavat uuden haaran lohkoketjuun. Mikäli ohjelmakoodiin tehtävät muutokset muodostavat protokollasta ei taaksepäin yhteensopivan version, eli protokollan toiminta muuttuu jollain tapaa olennaisesti, on kyseessä ns. *kova haarautuminen* (engl. hard fork). Tällöin noodit ja louhijat joutuvat tekemään valinnan, kumpaa versiota (haaraa) haluavat ylläpitää. Mikäli ohjelmakoodia muokataan niin, että Bitcoinin historian aikana on toteutettu useampia tarkoituksellisia haaraumia, joista yksi esimerkki on Bitcoin Cash. Tällöin Bitcoin Cashiksi nimetyn haaran lohkokokoa muutettiin merkittävästi lisäten transaktiokapasiteettia [12]. Mikäli kyseessä on taaksepäin yhteensopiva päivitys, on kyse pehmeästä haaroituksesta. Tällöin noodien ei ole välttämätöntä ottaa päivitettyä ohjelmistoa käyttöön. [4]

Shatoshi Nakamoton tarkoituksena oli rakentaa vaihtoehto nykyiselle keskitetylle valuutta- ja maksujärjestelmille. Hän ajatteli, että vain luopumalla keskitetystä vallasta, olisi millään uudella järjestelmällä merkitystä. Bitcoin osoitti lohkoketjuteknologian ja sen hajautetun soveltamisen olevan teknisesti mahdollista. Bitcoin itsessään tarjosi rajallisen määrän hajautetun teknologian sovelluskohteita, mutta avasi monen kehittäjän silämät uusille mahdollisuuksille. [4]

2.2 Toinen sukupolvi: Ethereum

2.2.1 Ethereum innovaationa

Vuonna 2014 venäläissyntyinen Vitalik Buterin julkaisi Ethereum-protokollaa kuvaavan *valkoisen kirjan* (engl. white paper) ja laajensi sitä, miten lohkoketjun soveltamismahdollisuudet konkreettisesti nähtiin. Paperi esitteli kuvauksen Ethereum-lohkoketjualustasta, jolla voitaisiin toteuttaa hajautettuja sovelluksia älysopimusten avulla. [5]

Älysopimus (engl. smart contract) on digitaalisesti määritetystä lupauksesta ja lupauksen täyttämismekanismista muodostunut kokonaisuus, joka visioitiin jo vuonna 1996 [13]. Ethereum oli kuitenkin ensimmäinen sovellus, joka teki visiosta laajaalaisesti todellisuutta mahdollistaen älysopimusten toteuttamisen ilman keskitettyä välimiestä. Käytännössä älysopimus on lohkoketjun päällä suoritettava ohjelmistosovellus, joka vastaanottaa pyyntöjä ja jonka suorituksen tulokset tallennetaan lohkoketjulle [14]. Ohjelma suoritetaan lohkoketjulla, eli sen suoritus ei tapahdu millään yksittäisellä palvelimella. Älysopimusten varaan rakennettuja sovelluksia kutsutaankin *hajautetuiksi sovelluksiksi* (engl. decentralized application, dApp).

Älysopimukset ja hajautetut sovellukset jatkavat bitcoin-valuutan aloittaman virtuaalisen käteisen perintöä ja mahdollistavat erityisesti erilaisten rahaliikenteeseen liittyvien palvelujen toteuttamisen hajautetusti. Voimakas painotus on ideaalissa, jossa välimiesten poistamisella saadaan lisättyä tehokkuutta ja avoimuutta sekä vähentämään keskitettyjen toimijoiden valtaa. Hajautetut sovellukset ovat käytännössä aina avointa lähdekoodia, sillä lohkoketjun data ja siten myös lohkoketjulle tallennetun sovelluksen lähdekoodi on julkista. Koska sovellukset pyörivät hajautetusti vertaisverkon päällä, on niillä myös hyvin alhaiset häiriöajat. Samasta syystä ne ovat myös äärimmäisen vastustuskykyisiä sensuroinnille. [5]

Sovelluksia on kehitetty hyvin monenlaisia, mutta merkittävä osa näistä liitty-

vät ns. *hajautettuun talouteen* (engl. decentralized finance, DeFi) ja mahdollistavat talousjärjestelmän perustoiminnallisuuksien tarjoamisen ohjelmallisesti. Näistä esimerkkejä ovat *automaattisten markkinatakaajien* (engl. automated market maker, AMM) päälle rakennetut täysin automatisoidut ja hajautetut kryptovaluuttapörssit [15], automaattiset lainapalvelut [16] sekä hajautetut varainhoitopalvelut [17]. Näiden lisäksi jatkuvasti kehitetään esimerkiksi pelejä ja sosiaalisen median sovelluksia.

2.2.2 Ethereumin toimintaperiaate

Vaikka Bitcoin mahdollistikin hajautetut virtuaalivaluutan transaktiot luotettavasti ja se tuki alkeellisia skriptipohjaisia "älysopimuksia", nosti Buterin esiin toteutuksen merkittäviä rajoitteita ja kehityskohteita, joita Ethereum ratkaisisi: Turing-yhteensopivuuden puute, sokeus lohkoketjun ominaisuuksia kohtaan, arvostuksen näkymättömyys sekä tilan seurannan puute. [5]

Turing-yhteensopivalla tarkoitetaan ongelmaa, joka on ratkaistavissa Turing-koneella. Lähes kaikki ohjelmointikielet ovat Turing-yhteensopivia, jolloin niitä kutsutaan Turing-kokonaisiksi. Käytännössä Turing-kokonaisuus määrittää, mitä voidaan toteuttaa algoritmisella laskennalla. Käänteisesti, mikäli ohjelmointikieli ei ole Turing-kokonainen, tiedetään sillä olevan laskennallisia ongelmia, joita ei voida ratkaista [18]. Toisin kuin Bitcoinin skriptikieli, oli Ethereumin älysopimuksiin käytettävä Solidity-ohjelmointikieli Turing-kokonainen, mikä merkittävästi laajensi lohkoketjun päälle rakennettavien ohjelmien moninaisuutta ja helpotti niiden ohjelmointia. [5]

Ethereum mahdollisti myös Bitcoinia monipuolisemman informaatiosisällön transaktioissa ja älysopimuksissa. Ohjelmat saattoivat viitata transaktioiden rakenneosiin, kuten aiemman transaktion tiivisteeseen tai satunnaismuuttujaan (nonce) tarjoten ohjelmoijille erinomaisen lähteen satunnaisuudelle. Samaten transaktioiden arvojen ei tarvinnut olla staattisia, vaan siirrettävän valuutan määrä saatettiin asettaa

dynaamisesti ohjelmalogiikan mukaan suoritushetkellä. [5]

Tilan seurannan puutteella Buterin tarkoitti, että Bitcoin-transaktiot olivat binäärisiä; transaktion kohteena olevat bitcoin-rahakkeet joko (a) siirrettiin tai (b) ei siirretty. Bitcoin-skriptien avulla ei voitu tallentaa minkäänlaista muuta ohjelman vaihetta tai tilaa, joten monivaiheisten tai valintoja sisältävien älysopimusten kehittäminen oli mahdotonta [5]. Ethereum transaktiot mahdollistavat tilanmuutoksen ja Ethereum-verkon eräs olennaisimmista tarkoituksista on ylläpitää kunkin tilin ja ohjelman tilaa. Ethereum-lohkoketjua ei yleensä kutsuta hajautetuksi tilikirjaksi, vaan kirjaimellisesti *hajautetuksi tilakoneeksi* (engl. distributed state-machine) [19]. Tämä oli ehkä merkittävin yksittäinen parannus, jonka Ethereum mahdollisti suhteessa esikuvaansa.

Ethereum oli pinnallisesti samankaltainen työtodistus-lohkoketju, kuin Bitcoin muodostuen louhijoiden ja varmentajien noodiverkostosta. Kuitenkin siinä missä Bitcoin-verkon UTXO-tietomallista oli johdettavissa vain tietoa eri *osoitteiden* (engl. address) bitcoin-katteista, voitiin Ethereum-verkossa siirtää ja tallentaa moninaisempia tietoja tilasta. Tilatieto muodostuu objektista, jota kutsutaan *tiliksi* (engl. account). Tilillä on neljä yksilöivää attribuuttia: (a) juokseva järjestysluku, joka ilmaisee tilin lähettämien transaktioiden lukumäärän, (b) tilin kate ether-valuutassa, (c) tilin mahdollisesti sisältämän älysopimuksen *tavukoodi* (engl. bytecode) ja (d) viittaus tilin tallennuskapasiteetin sijaintiin Ethereumin tietorakenteessa (engl. storageRoot) [20].

Ethereum-tilejä on kahta tyyppiä: (a) *ulkoisesti omistettuja tilejä* ja (b) lohkoketjun sisäisiä *sopimustilejä* (engl. contract account). Ulkoisesti omistetulla tarkoitetaan tiliä, jota hallitaan yksityisellä avaimella samaan tapaan kuin Bitcoin-verkossa. Käytännössä sitä hallitsee ihminen ja siltä voidaan lähettää transaktioita ja viestejä, mikäli ne valtuutetaan yksityisellä avaimella. Sopimustilit muodostavat hajautettujen sopvellusten ytimen, sillä ne ovat tilejä joihin on liitetty älysopimus. Kyseinen

älysopimus suoritetaan joka kerta, kun tili vastaanottaa viestin. [5]

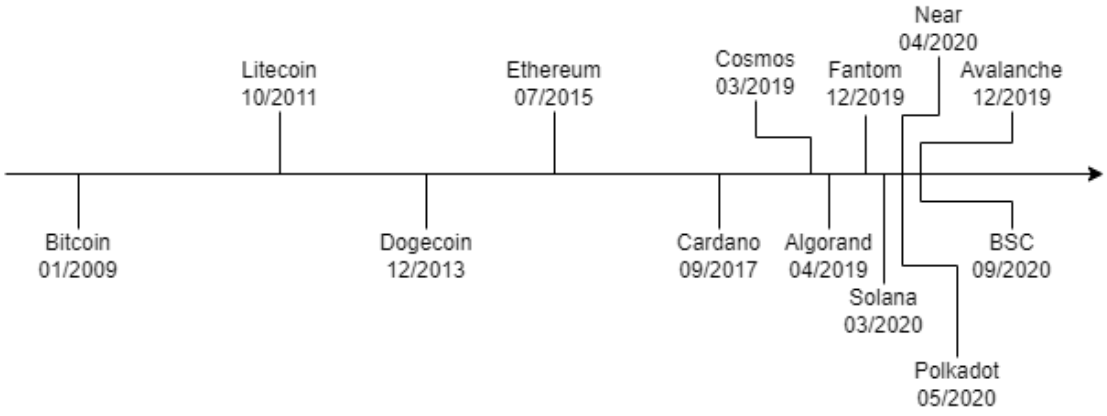
Ethereum-lohkoketjun transaktioita kutsutaan *viesteiksi* (engl. message). Viestejä voivat lähettää sekä ulkoisesti omistettujen tilien haltijat että älysopimukset. Viestit voivat sisältää siirrettävän valuuttamäärätiedon lisäksi muuta dataa. Tämän lisäksi mikäli viestin vastaanottaja on sopimustili ja älysopimus, voi se lähettää vastausviestin. Viestit käytännössä tukevat aliohjelmien syötteiden ja tulosteiden välittämistä. Myös transaktio-termiä käytetään Ethereum-kontekstissa, mutta sillä viitataan lähinnä lähetystä odottavaan datapakettiin, joka sisältää viestin. Muita rakenneosia transaktiossa ovat viestin vastaanottaja, lähettäjän kryptografinen allekirjoitus, lähetettävän ether-valuutan määrä ja lähetettävä data sekä kaksi transaktiokuluihin vaikuttavaa muuttujaa: (a) *STARTGAS* ja (b) *GASPRICE*. [5]

Koska Ethereumin älysopimukset tukevat esimerkiksi silmukoita, on alustassa oltava mekanismi estämään ikuisesti suoritettavat ohjelmat. Louhijoille maksettavan palkkion lisäksi itse älysopimuksien suorittamisella on kustannus. Käytännössä kussakin transaktiossa on määritelty STARTGAS-muuttujaan suoritettavien ohjelmavaiheiden maksimimäärä sekä GASPRICE-muuttujaan yksittäisen ohjelmavaiheen suorittamisen kustannus. Mikäli yksittäisen transaktion valtuuttavalta tililtä loppuu "polttoaine", eli ether, ennen älysopimuksen suorittamista loppuun asti, palautetaan ennen suorituksen aloittamista vallinnut tila. Transaktiokulut menetetään, vaikka älysopimuksen suorittaminen keskeytyisi ja epäonnistuisi. [5]

Syyskuuhun 2022 mennessä Ethereumin päälle onkin rakennettu tuhansia sovelluksia, joihin lukeutuu lukuisia täysin uudenlaisia ja vain lohkoketjuteknologialle ominaisia konsepteja [21]. Ethereumin ollessa ensimmäinen älysopimusalusta, on sille ehtinyt vuosien kuluessa rakentua vahva ekosysteemi. Lohkoketjuteknologian kehitys ja innovointi ei kuitenkaan päättynyt Ethereum-verkon käynnistymiseen 2015, vaan sen jälkeen on syntynyt kymmeniä vertailukelpoisia, teknisesti erittäin kehittyneitä vaihtoehtoja hajautetuksi älysopimusalustaksi.

2.3 Kolmas sukupolvi: Eth-killers

Bitcoin ja Ethereum syntyivät molemmat oman kategoriansa ensimmäisinä ja molemmat protokollat ehtivät saavuttaa merkittävän *ensimmäisen liikkujan edun* (engl. first mover advantage. Pitkään säilynyt etu oli saavutettavissa erityisesti siksi, että Vuonna 2009 lohkoketjukehitys ja vuonna 2015 älysopimusten kehitys olivat vielä lasten kengissään. Kyseisten teknologioiden ja markkinan kehitys oli verrattain hidasta, jolloin uuden innovaation on helpompi saavuttaa merkittävä ja kestävä etu. Vuoteen 2022 mennessä toiminnan määrä sektorilla on moninkertaistunut. Koska lohkoketjujen sekä markkina että teknologiat kehittyvät vauhdilla on erityisesti pitkään kestävän ensimmäisen liikkujan edun ylläpitäminen hyvin epätodennäköistä, vaikka se lyhyellä välillä vielä onnistuisikin. [22]



Kuva 2.3: Aikajana suosittujen L1-lohkoketjujen käynnistymisajankohdista

Uudet ensimmäisen asteen lohkoketjuprotokollat tavoittelevat yleensä aikaisempien lohkoketjuprojektien puutteiden korjaamista, jotka kulminoituvat *lohkoketjutrilemman* konseptiin. Trilemmalla tarkoitetaan sitä, että lohkoketjuteknologialla voitaisiin kerralla valita vain kaksi kolmesta kriittisestä ominaisuudesta: (a) hajautus, (b) turvallisuus ja (c) skaalautuvuus [23]. Käytännössä kukin lohkoketjuprotokolla tekee erilaisia kompromisseja trilemman suhteen toteutuksessaan ja vain tulevaisuus

kertoo, kenen näkemys voittaa. Tutkimuksen kolmannessa luvussa tarkastellaankin tarkemmin eri L1-protokollien elementtejä, joiden avulla eri protokollien eroja on helpompi hahmottaa.

3 L1-lohkoketjujen ominaisuudet

Tässä luvussa tarkastellaan tarkemmin L1-lohkoketjuille olennaisia ominaisuuksia, joiden avulla eri L1-lohkoketjujen välisiä eroja voidaan havainnollistaa. Luvun tarkoituksena on erityisesti pohjustaa kyselytutkimusta ja varmistaa, että lukija ymmärtää eri elementtien merkityksen yleisellä tasolla. Luvussa läpikäytävä lohkoketjujen vertailtavien ominaisuuksien listaus ei ole kattava ja myös happanee ajan kuluessa, sillä uudet innovaatiot määrittelevät pelikenttää jatkuvasti uudelleen. Tarkasteluun on kuitenkin valittu ominaisuuksia, millä protokollat ovat pyrkineet korostamaan oman olemassaolonsa ja kehityksensä merkitystä sekä millä ne ovat pyrkineet erottautumaan edeltäjistään ja kilpailijoistaan. Ominaisuuksia kuvattaessa eri lohkoketjuja ei ole vertailtu kattavasti, vaan kunkin ominaisuuden tai elementin kohdalla tiettyjä lohkoketjuja on nostettu havainnollistavina esimerkkeinä.

Osiossa 3.1 käsitellään eri L1-lohkoketjujärjestelmien konsensusmekanismeja, jotka käytännössä määrittelevät merkittävän osan kyseisten ekosysteemien teknisistä ominaisuuksista.

Osiossa 3.2 tarkastellaan eri L1-lohkoketjuprotokollien suorituskykyeroihin vaikuttavia elementtejä skaalautuvuuden näkökulmasta. Skaalautuvuudella käytännössä tarkoitetaan protokollan kykyä ylläpitää toimivaa järjestelmää käyttäjämäärien ja siten transaktioiden määrän kasvaessa.

Osiossa 3.3 tarkastellaan eri L1-lohkoketjuprotokollien turvallisuuteen liittyviä elementtejä. Koska lohkoketjujen toiminnan yhtenä peruskivenä on mahdollistaa

toiminta ilman luotettavia välimiehiä, on protokollien hajautuksen taso ja menetelmät sen saavuttamiseksi merkittäviä.

Osiossa 3.4 tarkastellaan eri L1-lohkoketjuprotokollien aktiivisuutta erityisesti protokollien käytön ja kehityksen mukaan. Eri lohkoketjuprotokollia voidaan pitää käytännössä kilpailevina teknologioina ja teknologia-alustoina, joten on hyvin merkityksellistä hahmottaa eroja esimerkiksi käyttäjämäärien, protokollan varaan rakennettujen sovellusten ja palveluiden, protokollaan sidotun pääoman ja protokollan kehittäjien määrien suhteen.

Osiossa 3.5 tarkastellaan L1-lohkoketjuprotokollien maineeseen liittyviä elementtejä.

3.1 Lohkoketjujen konsensusmekanismit

Tässä kappaleessa tarkastellaan eri kehitettyjen L1-lohkoketjujärjestelmien konsensusmekanismeja, jotka käytännössä määrittelevät merkittävän osan kyseisten ekosysteemien teknisistä ominaisuuksista. Kuten aikaisemmissa luvuissa on käyty läpi, on konsensuksen saavuttaminen eräs lohkoketjun olennaisimmista rakenneosista. Menetelmät konsensuksen saavuttamiseen eroavat eri protokollien välillä merkittävästi. Eri mekanismeja on kehitetty monia, kuten auktoriteettitodistus (engl. Proof of Authority, PoA) ja tilatodistus (engl. Proof of Space) [24]. Tässä osiossa keskitytään erityisesti tunnetuimpiin ja yleisimpiin mekanismeihin, eli työtodistukseen (engl. Proof of Work, PoW) ja varantotodistukseen (engl. Proof of Stake, PoS).

3.1.1 Työtodistus

Työtodistus (engl. proof-of-work, PoW) on ensimmäinen ja tunnetuin lohkoketjujen konsensusmekanismi, jota käyttävät mm. Bitcoin- ja Litecoin-lohkoketjut [4] [25]. Konsensusmekanismin toimintaperiaatetta on kuvattu tarkemmin luvussa 2.1. Vaik-

ka työtodistus-konsensusmekanismi on todettu toimivaksi menetelmäksi hajautetun lohkoketjualustan toteuttamiseksi, on siinä myös varjopuolia. Eräs ilmeisimmistä on sen merkittävä energiankulutus. Jatkuva louhijoiden välinen kilpailu uusien lohkojen louhimisessa johtaa jatkuvasti suurempaan laskentatehon uhraamiseen. Jo vuoden 2017 aikana Bitcoin-verkon louhijoiden arvioitiin kuluttavan energiaa noin 8,3 biljoonaa kilowattituntia, joka vastaisi noin Panaman tai Angolan valtioiden kokonaiskulutusta samana vuonna [26]. Vaikka louhintalaitteiston energiatehokkuus on kasvanut vuosien varrella, on mm. Bitcoin-louhintaan käytetyn laitteiston tiivistefrekvenssi kasvanut monta kertaluokkaa. Joulukuun 2017 lopussa louhijat laskivat keskimäärin 13 kvadriljoonaa tiivistefunktiota sekunnissa. Vuoden 2022 lokakuun alussa Bitcoin-verkon tiivistefrekvenssi oli saavuttanut 228 kvadriljoonan tiivistefunktion sekuntivauhdin [27].

3.1.2 Varantotodistus

Jo hyvin aikaisessa vaiheessa työtodistusprotokollille on pyritty kehittämään energiatehokkaampaa vaihtoehtoa ja aiheesta on käyty keskustelua Bitcoin-harrastajien parissa jo vuodesta 2011 [28]. Pseudonyymi Sunny King julkaisi 2012 lohkoketjun, Peercoinin, jonka varantotodistusmenetelmällä (engl. proof of stake, PoS) voitaisiin korvata työtodistusmekanismi. Kingin varantotodistusmenetelmässä keskeistä on raha-ajan käsite (engl. coin age), jonka avulla määritettiin kuka uuden lohkon saa luoda ja siten kerätä lohkopalkkion. Raha-aikaa laskettiin osoitekohtaisesti kertomalla hallussa olevien rahakkeiden määrä säilytetyn ajan pituudella. Suurimman raha-ajan kerryttänyt sai lunastaa uuden lohkon lyömisoikeuden. Vaikka Peercoin-verkko käyttikin pääosin varantotodistusmekanismia, oli sen konsensusmekanismi eräänlainen hybridimalli. Se hyödynsi toimintansa alkuvaiheessa myös työtodistusmekanismia rahakkeiden reilumpaan ja tasaisempaan jakamiseen. [29]

Ensimmäisen kokonaan varantotodistuksen varassa toimiva lohkoketju, eli loh-

koketju jonka konsensusmekanismiin viitataan myös puhtaana varantotodistuksena (engl. pure proof of stake, PPoS), oli NXT. Vuonna 2013 julkaistun NXT:n toimintaperiaatteessa unohdettiin raha-ajan käsite ja sen sijaan uuden lohkon lyömisoikeudet jaettiin satunnaisesti niiden varmentajien välille, jotka olivat maksaneet pantin (engl. stake). Todennäköisyys saada lyömisoikeus jakautui pantin suhteellisen suuruuden mukaan. [30] Hyvin samankaltaista konsensusmekansimia käytettiin mm. Blackoin-lohkoketjun konsensuksen muodostamiseen [31].

Daniel Larimerin vuonna 2013 esittelemä valtuutettu varantotodistus (engl. delegated proof of stake, DPoS) oli nopeampi, kuin senhetkiset työtodistus- ja varantotodistuskonsensuksia käyttävät lohkoketjut. Se myös lisäsi mahdollisuuden rahakkeiden haltijoille valtuuttaa tai äänestää kolmannen osapuolen varmentaja edustamaan heitä uuden lohkon muodostamisessa [32]. Äänestetyt varmentajat loivat lohkoja vuorotellen ja maksoivat vastaanotetuista lohkopalkkioista osuudet takaisin heidät äänestäneille rahakkeiden omistajille valtuutuksien yhteydessä annettujen panttien suhteessa. Käytännössä koska lohkoketjun varmentajana toimiminen vaatii aina tiettyä teknistä kyvykkyyttä ja sopivaa laitteistoa, mahdollistaa valtuutettu varantotodistus myös alhaisemman kynnyksen osallistumisen lohkoketjun varmentamiseen ja siten myös lohkopalkkioiden kerryttämiseen. Valtuutettua varantotodistusta konsensusmekanismina käyttävät eri lohkoketjut, kuten EOS [33] ja Tron [34].

King ennusti vuonna 2012 oikein arvioidessaan, että varantotodistus tulee yleistymään työtodistusta merkittävästi [29]. Varantotodistuskonsensuksesta kehitettiinkin edelleen seuraavina vuosina useita versioita, jotka kukin pyrkivät ratkaisemaan edeltäjiensä puutteita uusilla menetelmillä. Ethereumin kehittäjien Casper-protokollan mukaan varmentajiksi sai ryhtyä kuka vain tarpeeksi suuret vakuudet pantannut. Epärehellisiä tai suorituskyvyltään puutteellisia varmentajia rankaistiin tuhoamalla (engl. slashing) osa vakuuksista [35]. Cardano-lohkoketjun Ouroboros-konsensus esitteli palkkiomekanismin, joka palkitsi rehellisiä validaattoreita ja esti stake grin-

ding -nimisen turvallisuuspuutteen [36]. Muita esimerkkejä varantotodistuksen variaatioista ovat kymmenien muiden joukossa mm. Cosmos-verkoston Tendermint [37] ja Polkadot-lohkoketjun nimitetty varantotodistus (engl. nominated proof of stake, NPoS) [38].

Konsensusmekanismit ovat L1-lohkoketjujen kehittäjille tärkeitä, sillä ne sanelevat merkittävän osan lohkoketjujen teknisistä ominaisuuksista ja vastaavat kysymykseen "miksi". Ne eivät kuitenkaan kerro mihin lohkoketjujen suorituskyky käytännössä asettuu ja lopulta kysymykseen "mitä"voidaan vastata vain tarkastelemalla muita ominaisuuksia.

3.2 Lohkoketjujen skaalautuvuus

Bitcoinia ja muita kryptovaluuttoja on verrattu sähköiseen käteiseen, sillä lohkoketju on mahdollistanut transaktioiden tekemisen ja arvon siirtämisen tahojen välillä ilman luotettua välimiestä. Samaan tapaan, kuin seteli tai kolikko vaihtaa fyysisesti omistajaa, voidaan esimerkiksi BTC-valuuttaa siirtää vertaisverkossa digitaalisesti yksilöltä toiselle. Arvon siirtäminen on ollut lohkoketjuteknologian syntymästä asti sen merkittävimpiä sovelluskohteita ja monen kryptovaluutan kehittäjän ja käyttäjän visiona on ollut tarjota toimiva vaihtoehto nykyisen keskitetyn maksunsiirtojärjestelmän tilalle. Jotta mikään sovellus voisi edes teoriassa olla toimiva vaihtoehto nykyisille sähköisille maksujärjestelmälle, kuten Visalle, Mastercardille ja SWIFTille, tulisi sen kyetä käsittelemään kaikkien sen käyttäjien tekemät transaktiot. Tällaisen vision toteutuminen vaatii merkittävää suorituskykyä ja skaalautuvuutta.

Lohkoketjujen skaalautuvuuteen liittyvät ongelmat voidaan yleisesti jakaa kahteen kategoriaan; (a) transaktiokapasiteettiin ja (b) hintaan. Transaktiokapasiteetin ensisijainen mittari on transaktionopeus, johon lohkoketju kykenee. Toissijaisesti kapasiteettiin liittyy myös tallennuskapasiteettiin liittyvät kysymykset. Jos lohkoketjuun tallennetaan rajoittamatta kaikki transaktioihin liittyvä data, kasvattaa se

merkittävästi verkon ylläpitäjien teknisiä vaatimuksia ja siten kustannuksia. Transaktioiden kustannukset eivät myöskään saisi olla kovin korkeita, että hinta ei karkota käyttäjiä. [39]

3.2.1 Transaktionopeus

Transaktionopeudesta käytetään yleisesti yksikköä *transaktioita per sekunti* (engl. transactions per second, TPS). Maksuvälittäjä Visa käsittelee keskimäärin noin 1700 ja Paypal noin 200 transaktiota sekunnissa [40]. Vakiintuneimmat lohkoketjuprotokollat, eli Bitcoin ja Ethereum, kykenevät toistaiseksi käsittelemään vain murto-osan keskitettyjen järjestelmien käsittelemien transaktioiden lukumäärästä. Bitcoin kykenee keskimäärin käsittelemään noin neljä transaktiota sekunnissa ja Ethereumin noin 20 transaktiota sekunnissa [40]. Myöhemmin kehitetty Solana-lohkoketju käsitteleekin jo monta mittaluokkaa suurempia määriä transaktioita noin 4000 transaktion sekuntivauhdilla [41]. Transaktioiden lukumäärän mukaan laskettu suorituskyky ei yksinään kuitenkaan ole riittävä mittari määrittelemään lohkoketjujen keskinäistä paremmuutta.

Lohkoketjun suorituskykyyn eli transaktionopeuteen vaikuttavat kolme keskeistä tekijää: (a) *lohkon koko* (engl. block size), (b) *lohkoaika* (engl. block time) ja (c) *transaktioiden varmennusaika* (engl. transaction finality). Lohkon transaktionopeus on perustavanlaatuinen osa eri lohkoketjujen suunnittelua ja sillä on merkittävä välillinen vaikutus lohkoketjun hajautuksen määrään. Käytännössä transaktionopeuden kasvattaminen lisää lineaarisesti tarvetta transaktiohistorian tallennuskapasiteetille, joka asettaa haasteita lohkoketjun hajautuneisuuden varmistamisessa. Hajautuksen näkökulmasta asiaa tarkastellaan tarkemmin osiossa 3.4.

Lohkon koko

Lohkon koko määrittelee kuinka monta transaktiota kokonaisuutena mahtuu yhteen uuteen lohkoketjun lohkoon, eli käytännössä kuinka monta transaktiota voidaan suorittaa kerralla. Suuremmat lohkokoot tarkoittavat suurempaa määrää kerralla suoritettavia ja kerralla lohkoketjuun tallennettavia transaktioita. Transaktiot suoritetaan samalla hetkellä, kun uusi lohko luodaan ja liitetään ketjuun. Ketjuun lisättävän lohkon koko on suoraviivaisin muuttuja, jolla voidaan vaikuttaa lohkoketjun suorituskykyyn. Lohkon koon kasvattaminen ei kuitenkaan välttämättä lisää lohkoketjun suorituskykyä lineaarisesti, sillä suuremmat lohkokoot todennäköisesti lisäävät myös epäonnistuneiden transaktioiden lukumäärää [42].

Käynnistyessään Bitcoin-lohkoilla ei ollut erikseen määritettyä lohkon kokorajoitusta, joskin silloinen bitcoinin pääkehittäjä Satoshi Nakamoto päätyi 1 MB rajan pian määrittelemään. Bitcoinin myöhemmän historian aikana lohkojen kokoa on muutettu. Vuonna 2017 SegWit -protokollapäivityksessä 1 MB kiinteä kokorajoitus muutettiin transaktioiden *kokonaispainorajaksi* (engl. weight limit), jonka teoreettinen maksimisuuruus on 4 MB, joskin käytännössä keskimäärin 2 MB [[BIP-141]]. Bitcoin Cash, joka on kilpaileva *haarauma* (engl. hard fork) Bitcoinista, aloitti toimintansa vuonna 2017 ainoana käytännön eronaan juurikin suurempi 8 MB lohkokoko. Se päivitetiin 2022 käyttämään 32 MB lohkokokoa ja on näin transaktiokapasiteetiltaan merkittävästi suurempi, kuin Bitcoin.

Kaikissa lohkoketjuissa lohkon suuruutta ei määrää kiinteä kokorajoite. Esimerkiksi älysopimuksia tukevan Ethereum-lohkoketjun lohkojen suuruuden määrää dynaaminen *kaasuraja* (engl. gas limit). Erilaiset älysopimukset kuluttavat eri määriä kaasua riippuen niiden rakenteesta ja monimutkaisuudesta. Ethereum-järjestelmä pyrkii tuottamaan 15 miljoonan kaasuyksikön lohkoja, joskin raja kasvaa kysynnän kasvaessa aina 30 miljoonaan kaasuyksikön rajaan. [43]

Lohkoaika ja varmennusaika

Lohkoaika määrittelee frekvenssin, miten usein lohkoketjuun luodaan uusia lohkoja ja siten myös suoritetaan uusia transaktioita. Lohkoaika on se aika, joka kuluu lohkoketjun louhijoilta ja/tai validaattoreilta uuden lohkon löytämiseen, transaktioiden koostamiseen lohkoon ja sen julkaisemiseen.

Lohkoaika vaihtelee merkittävästi lohkoketjuttain. Esimerkiksi Bitcoin-verkon lohkoaika on keskimäärin 10 minuuttia ja Ethereum-verkossa 12 sekuntia [44].

Varmennusajalla tarkoitetaan aikaa, joka kuluu uuden lohkon julkaisemisen jälkeen ennen sen hyväksymistä virallisesti osaksi ketjua. Käytännössä kullekin lohkoketjulle on määritelty tietty lukumäärä lohkoja, jotka on liitettävä ketjuun varmennettavan lohkon jälkeen. Tällä mekanismilla käytännössä määritellään verkon käyttäjille ja sovelluksille yhteinäinen tapa määrittää verkon tila, vaikka tapahtuisi haaraumia.

3.2.2 Transaktiokustannukset

Yleisesti *transaktiokustannuksella* (engl. transaction cost) tarkoitetaan lohkoketjulla tehtävien muutosten, kuten valuutan siirtämisen tai älysopimuksen suorittamisen, kustannusta. Eri lohkoketjuilla on erilaisia mekanismeja määritellä transaktiokustannusten suuruus, mutta yleisesti ne ovat suoraan verrannollisia lohkoketjun transaktiokapasiteettiin ja käyttäjien kysyntään tehdä transaktioita. Mikäli kysyntä ylittää kapasiteetin, kasvavat transaktiokustannukset.

Eri lohkoketjujen transaktiokustannusten tasot vaihtelevat merkittävästi. Taloudessa alhaiset transaktiokustannukset edesauttavat talouskasvua, kun taas korkeat kustannukset hidastavat sitä [45]. Tämä johtaa lohkoketjuissa siihen, että lohkeketjut joiden transaktiokustannukset ovat alhaisempia, lisäävät vaihdantaa ja myös mahdollistavat transaktiointensiivisten sovellusten, kuten pelien, kehittämisen.

Koska transaktiokustannukset maksetaan aina kunkin lohkoketjun omalla natii-

virahakkeella, kasvaa transaktiokulujen valuuttamääräinen (esim. suhteessa euroon) arvo natiivirahakkeen arvon kasvaessa.

3.2.3 Skaalautuvuusratkaisut

Lohkoketjujen suorituskyvyn parantaminen on haastavaa. Vaihtoehtona on yleensä tehdä muutos itse lohkoketjuun eli ns. *ketjulla* (engl. on-chain) tai siirtää transaktio tai transaktion osa suoritettavaksi *ketjun ulkopuolelle* (engl. off-chain). Ketjulla tehtävät yksinkertaiset muutokset, kuten lohkokoon kasvattaminen, tuovat mukanaan yleensä lieveilmiöitä, kuten virheherkkyyttä tai verkon ylläpidon kustannusten nousua, jolloin haitat ylittävät muutoksen hyödyt [42]. Kokonaisuutena hyödylliset ratkaisut ovatkin yleensä teknisesti hyvin monimutkaisia ja erittäin tapauskohtaisia. Esimerkkejä ketjulla tehdyistä skaalausparannuksista ovat Bitcoin-lohkoketjun Segwit-päivitys [46] ja Ethereumin Sharding [47]. Segwit muutti Bitcoin-transaktioiden teknistä rakennetta eriyttämällä allekirjoitusdatan erilliseen datarakenteeseen lisäten transaktiokapasiteettia ja turvallisuutta. Shardingin avulla lievennettiin yksittäisten ylläpitäjänoodien datan tallennusvaatimuksia. [39]

L1-lohkoketjuun kohdistuvaa transaktiopainetta voidaan lieventää siirtämällä transaktioita suoritettavaksi ketjun ulkopuolella. Käytännössä tämä tarkoittaa, että lohkoketjuun on kytketty ulkoinen sovellus tai toinen, yleensä suorituskyvyltään parempi, lohkoketjuverkko. Tällaista yhteenkytkettyä lohkoketjua kutsutaan yleisesti *toisen asteen lohkoketjuksi* (engl. layer 2) eli L2-lohkoketjuksi. L2-lohkoketjut ovat riippuvaisia L1-lohkoketjujen turvallisuusinfrastruktuurista ja toimivat eräänlaisena kerroksena L1-ketjun päällä. Koska L2-lohkoketjulla tehtävät transaktiot ovat yleensä halvempia, kannattaa esimerkiksi transaktiointensiivisiä sovelluksia, kuten pelejä, toteuttaa L2-ketjulla. Pelien ja sovellusten lopputulokset välitetään tallennettavaksi L1-lohkoketjulle. [48]

3.3 Lohkoketjujen turvallisuus

Lohkoketjuteknologiaan liittyy konseptuaalisesti toimintavarmuus, sillä sen kehittämisen tarkoituksena on ollut kyetä liikuttamaan internetin yli varallisuutta turvallisesti ilman välikäsiä. Se nojaa muutamiin hyvin tunnettuihin konsepteihin, kuten *julkisen avaimen järjestelmään* (engl. public key infrastructure, PKI), kryptografiseen salaukseen, tiedon avoimuuteen ja muuttumattomuuten sekä päätöksenteon hajautukseen [49]. Yleisesti lohkoketjuteknologia nojaa vahvasti kryptografiaan [50]. Julkisen avaimen järjestelmää, salausta, avoimuutta ja muuttumattomuutta on kuvattu lyhyesti osiossa 2.1.2.

3.3.1 Lohkoketjun hajautuksen taso

Päätöksenteon hajauttaminen on erittäin merkittävä lohkoketjujen turvallisuuteen vaikuttava elementti. Koska uusia lohkoja luodaan enemmistökonsensuksen avulla, voi vilpillinen toimija manipuloida totuutta omaksi edukseen, mikäli hallitsee yli 50% osuutta konsensuksen määrittelevästä resurssista (myöh. konsensusresurssi). Tällaista tilannetta kutsutaan *51% hyökkäykseksi* (engl. 51% attack) [11]. Mitä hajautuneemmin lohkoketjun konsensusresurssit ovat jakautuneet, sitä haastavampaa on saada määräenemmistöä louhijoita tai varmentajia vilpilliseen yhteenliittymään.

Eräs tapa, millä lohkoketjujen hajautuneisuutta on mitattu, on gini-kerroin [51] [52]. Gini-kerroin on taloustieteessä käytetty luku kuvaamaan miten tasaisesti tietty resurssi on jakaantunut populaatiossa. Lukema ilmaistaan vaihteluvälillä 0—1. 0 kuvaa tilannetta, jossa resurssi on jakautunut absoluuttisen tasan ja 1 tilannetta, jossa kaikki resurssit ovat yhdellä [53]. Lohkoketjujen osalta on mielekästä käyttää gini-kerrointa kuvaamaan päätöksenteon, eli konsensuksen saavuttamisen osalta merkitsevää resurssia. Esimerkiksi työtodistus-konsensusmekanismia käyttävien lohkoketjujen osalta relevantti konsensusresurssi on tiivistefrekvenssin jakauma louhijoiden välillä, joskin gini-kerroin voidaan muodostaa myös toteuman, eli louhittujen

lohkojen jakauman, perusteella [51]. Varantotodistus-konsensusmekanismia hyödyntävissä lohkoketjuissa merkitsevää on natiivirahakkeiden jakauma eri *varmentajien* (engl. validator) välillä [52]. Korkea gini-kerroin kertoo, että valta on keskitetympää ja siten pienempi lukumäärä epärehellisiä louhijoita tai varmentajia kykenisi manipuloimaan konsensustulosta onnistuneesti. Alhainen gini-kerroin vastaavasti viestii konsensusresurssien tasaisemmasta jakaumasta, jolloin konsensuksen manipuloimisen vaikeus nousee merkittävästi.

Taulukossa 3.1 on kuvattu eri varantotodistus-lohkoketjujen hajautuksen tasosta kertovia gini-kertoimia. Lukujen mukaan Cardano on vertailuryhmän eniten ja Elrond vähiten hajautettu.

L1-protokolla	Gini-kerroin
Cardano	0,61
Tron	0,67
Polkadot	0,78
Fantom	0,81
Cosmos	0,83
Avalanche	0,87
BSC	0,91
Elrond	0,92

Taulukko 3.1: Kahdeksan varantotodistukseen pohjautuvan L1-protokollan natiivirahakkeiden jakaantuminen 1000 suurimman lompakon kesken 16.12.2021. [52]

Hajautuksen suhteen pelkkä olemassaolevien konsensusresurssein tasainen jakautuminen ei ole riittävää lohkoketjun turvallisuuden ylläpitämiseksi, vaan merkitystä on myös volyymilla. Esimerkiksi työtodistus-lohkoketjujen osalta tällä tarkoitetaan louhintaan käytettyä tiivistefrekvenssiä. Jos tietyn lohkoketjun verkon tiivistefrekvenssi on alhainen, on vilpillisen toimijan suhteellisen helppoa ja edullista lisätä tarpeeksi paljon uutta laskentatehoa verkkoon ja siten saavuttaa määräenemmistö ja päätäntävalta [11].

Välillisesti louhijoiden tai validaattorien määrään vaikuttaa mm. lohkoketjun yksittäisen noodin ylläpidon kustannus. Mitä edullisempaa ja helpompaa on lohko-

ketjun noodin ylläpito ja esimerkiksi toimiminen louhijana tai varmentajana, sitä useampi toimija voi niin tehdä. Eri lohkoketjuilla on erilaiset tekniset vaatimukset noodin ylläpitoon. Esimerkiksi Avalanche-noodin ylläpitoon suositellaan tietokonetta, jossa on vähintään kahdeksan prosessoriydintä, 16 GB RAM-muistia ja 1 TB tallennustilaa. Tämän lisäksi vaaditaan 2000 AVAX-rahakkeen talletus [54]. Vastaavasti Solana-noodin ylläpitoon suositellaan tietokonetta, jossa on vähintään 16 suoritinydintä, 256 GB RAM-muistia ja 2 TB tallennustilaa, eli vaatimukset ovat merkittävästi suuremmat. Laitteiston ylläpidon lisäksi noodin ylläpitäjälle tulee 1,1 SOL-rahaketta kuluja päivittäin [55].

3.3.2 Lohkoketjun anonymiteetti

Toisin kuin yleinen harhaluulo on, pääosa lohkoketjuista eivät ole hyviä alustoja anonyymeihin transaktioihin. Vaikka esimerkiksi Bitcoin-verkossa luomishetkellä kaikki lohkoketjuosoitteet ovat anonyymejä ja osoitteen perusteella on mahdotonta päätellä, kuka sitä hallitsee, ovat kaikki lohkoketjun päällä tehdyt transaktiot julkisia. Analysoimalla kattavasti Bitcoinin transaktiohistoriaa, voidaan hyvinkin tehokkaasti kartoittaa valuuttavirjojen liikkeet ja jopa tunnistaa lähettäjä tai vastaanottaja. Tutkimus alalla on osoittanut, että sama pätee muihinkin lohkoketjuihin, jopa niihin jotka on erityisesti suunniteltu suojaamaan käyttäjiensä yksityisyyttä. Esimerkkejä tällaisista lohkoketjuista ovat Monero ja Zcash. [56]

Vaikka L1-lohkoketjut eivät ensisijaisesti takaa anonyymiytta, on niiden päälle rakennettu erilaisia yksityisyyttä lisääviä palveluita ja protokollia. Yksi tunnetuimmista on avoimeen lähdekoodiin perustuva transaktioiden sekoittaja Tornado Cash [57]. Toistaiseksi kuitenkin kryptovaluuttatransaktioiden anonyymiyden tulkitaan usein sotivan kansallista ja kansainvälistä rahanpesulainsäädäntöä vastaan, minkä toimesta esimerkiksi Tornado Cashin käyttö on mm. Yhdysvalloissa kriminalisoitu [58].

3.4 L1-ekosysteemien aktiivisuus

3.4.1 Käyttöaktiivisuus

Lohkoketjujen, kuten muidenkin ekosysteemien, elinvoimaisuutta voidaan arvoida seuraamalla miten aktiivisesti siellä toimitaan. L1-lohkoketjujen käyttöaktiivisuutta voidaan arvioida seuraamalla (a) transaktioiden määrää [59], (b) aktiivisten käyttäjien määrää ja (c) sovellusten määrää.

Koska lohkoketjujen transaktiot ovat julkisia, voidaan niiden lukumäärää seurata suoraviivaisesti. Eri lohkoketjujen transaktioiden lukumääriä voidaan verrata absoluuttisesti tai suhteessa transaktiokapasiteettiin. Yksittäiset transaktiot eivät kuitenkaan ole saman arvoisia keskenään, mikä vaikuttaa vertailtavuuteen. Esimerkiksi Solana-lohkoketjun konsensusmekanismiin liittyvät ns. *äänestystransaktiot* (engl. vote-transactions), jotka ovat tarpeellisia verkon toiminnassa, mutta eivät liity käyttäjien aktiivisiin toimenpiteisiin [60]. Transaktioiden määrää voidaan mitata myös laskemalla transaktioilla siirrettävää arvoa.

Lohkoketjujen käyttäjien arviointi ei ole aina suoraviivaista. Vaikka lohkoketjujen transaktiot ja siten lohkoketjujen osoitteet ovat julkisia, on hyvin haastavaa ja useimmiten mahdotonta määritellä kuka tiettyä osoitetta hallitsee ja yhdellä käyttäjällä voi olla useita rinnakkaisia osoitteita samalla lohkoketjulla. Käyttäjien aidon lukumäärän sijaan verrataan yleensä aktiivisten uniikkien osoitteiden lukumäärää. Aktiivisuudella tarkoitetaan sitä, että osoite on valtuuttanut transaktion tietyn aikaikkunan sisällä. Aikaikkunan pituus riippuu analyysin tekijästä.

Lohkoketjujen päälle rakennettujen hajautettujen sovellusten lukumäärän on suoraviivainen metriikka. Samaan tapaan kuin muutenkin ohjelmistokehityksessä ja alustataloudessa, suurempi määrä sovelluksia houkuttelee käyttäjiä ja indikoi suurempaa määrää kehitysaktiviteettia alustalla. Eri L1-lohkoketjuilla onkin merkittäviä eroja julkaistujen sovellusten lukumäärässä. Johtuen lohkoketjujen vaihtelevista

teknisistä ominaisuuksista, vaihtelevat lohkoketjujen edellytykset tukea tietyn tyyppisiä sovelluksia merkittävästi. Esimerkiksi Solana-lohkoketjun alhaiset transaktiokustannukset ja korkea transaktiokapasiteetti ovat houkutelleet paljon pelinkehittäjiä suhteessa muihin L1-verkkoihin.

3.4.2 Kehitysaktiivisuus

Kehitysaktiivisuus antaa välillisen keinon arvioida lohkoketjun tulevaisuuden edellytyksiä, sillä aktiivinen ohjelmistokehitys ja kehittäjien lukumäärä ennakoi käytettävien sovellusten määrän ja laadun paranemista. Tietyn lohkoketjuekosysteemin kehitysaktiivisuutta voidaan arvioida suoraan sen parissa toimivien kehittäjien lukumäärän perusteella. Tietyn teknologian parissa työskentelevien potentiaalista määrää voidaan entisestään arvioida eri ohjelmointikielten osaajien lukumäärän perusteella.

Kehittäjien määrä

Eri protokollien ja ekosysteemien parissa toimivien kehittäjien lukumäärä indikoi voimakkaasti niiden kehityksen suhteellista nopeutta ja esimerkiksi kehitettävien sovellusten lukumäärää. Kehitysaktiivisuuden muutokset kertovat erityisesti teknisesti orientoituneiden ihmisten huomion muutoksista eri lohkoketjuprojektien välillä.

Taulukossa 3.2 on kuvattu kehittäjämääriltään suurimmat L1-protokollat sekä muutos kehittäjien määrässä vuoden 2021 aikana.

L1-protokolla	12/2020	12/2021	Muutosprosentti
Ethereum	2980	3920	31,5%
Polkadot	840	1400	66,7%
Solana	181	878	385,1%
Bitcoin	617	673	9,1%
NEAR	100	410	310%
Cardano	190	370	94,7%
Binance Smart Chain	185	330	78,4%
Algorand	56	201	258,9%
Internet Computer	41	192	368,2%
Fantom	18	88	388,9%

Taulukko 3.2: 10 kehittäjämäärältään suurimman L1-protokollan kehittäjämäärämuutos vuoden 2021 aikana [61].

Ethereum on suurin lohkoketjuprotokolla kehittäjäaktiivisuudella mitattuna. Joulukuussa 2021 protokollan parissa toimi keskimäärin 3920 avoimen lähdekoodin kehittäjää, joka oli 31,5% enemmän, kuin vuotta aikaisemmin. Markkina-arvoltaan suurimmalla kryptoprotokollan Bitcoinin parissa toimi joulukuussa 2021 673 avoimen lähdekoodin kehittäjää, joka oli sekin 9,1% enemmän kuin vuotta aikaisemmin. Nopeimmin kehittäjämääriltään kasvaneet ovat kasvaneet Fantom, Solana ja Internet Computer -ekosysteemit, joiden kehittäjämäärät ovat miltei viisinkertaistuneet. [61]

Yleisesti lohkoketjuteknologioiden parissa työskentelevien ohjelmistokehittäjien lukumäärä on kasvanut viime vuosina merkittävästi. Ei ole yllättävää, että aktiivisten kehittäjien lukumäärä on kasvanut kryptomarkkinan markkina-arvon kasvaessa, mutta kehittäjien määrä on pysynyt tasaisena myös kryptovaluuttojen arvostusten romahtaessa. Joulukuussa 2021 kuukausittain aktiivisten kehittäjien määrä oli kasvanut yli 18000:een. [61]

Ohjelmointikielet

Kuten mitä vain ohjelmistoja, myös eri lohkoketjuprotokollia ohjelmoidaan ja toteutetaan eri ohjelmointikielillä. Ohjelmointikielen valintaan liittyy erityisesti sen sopivuus aiottuun tarkoitukseen, mutta myös tarjolla olevien ohjelmoijien osaaminen [62]. Tämä tarkoittaa sitä, että myös L1-protokollien tulevaisuuden kannalta sen kehitykseen valituilla ohjelmointikielillä voi olla merkittävä vaikutus protokollan menestykseen.

Lohkoketjuprotokollia kehitetään monilla eri kielillä, joista suosituimpia ovat Solidity, Go, Rust, ja C++. Juuri Solidity on korostunut lohkoketjukehityksessä, sillä se kehitettiin erityisesti Ethereumin älysopimusten kehittämistä varten pääkehittäjinään Christian Reitwiessner ja muita Ethereum-kehittäjiä [63]. Käytännössä kaikki EVM-yhteensopivien protokollien sovellukset ja älysopimukset kehitetään ensisijaisesti Solidity-kielellä. Lohkoketjuprojektit myös ovat oman aikansa tuotteita, sillä vanhemmat lohkoketjuprotokollat hyödyntävät useimmiten hieman vanhempia kieliä, kuten C, ja C++. Vastaavasti taas uudemmat projektit hyödyntävät paljon kieliä kuten Go ja Rust. [64]

Protokollat ja erityisesti niiden ympärille rakentuvat ekosysteemit ovat monimutkaisia kokonaisuuksia ja niiden eri osiin, kuten ydintoiminnallisuuksiin, älysopimuksiin, SDK:ihin tai sovelluksiin käytetään usein eri ohjelmointikieliä. On myös projekteja, joissa kaikki ekosysteemin komponentit on toteutettu pääosin yhdellä kielellä.

Taulukkoon 3.3 on koottu natiivirahakkeen markkina-arvon mukaan arvokkaimpien L1-protokollien kehityksessä käytettyjä ohjelmointikieliä.

L1-protokolla	Julkaisuvuosi	Ensisijaiset ohjelmointikielet
Bitcoin	2009	C++, Python
Litecoin	2011	C++,
Ripple	2012	C++, Typescript
Doge	2013	C++,
Stellar	2014	C, Go, Javascript
Monero	2014	C++,
Ethereum	2015	Go, Solidity
Vechain	2015	Go, Typescript
Cardano	2017	Haskell
Bitcoin Cash	2017	C++,
Tron	2018	Java
Theta	2018	Go, Solidity
Algorand	2019	Go, Typescript / Python
Fantom	2019	Go, Solidity
Binance Smart Chain	2020	Go, Solidity, Typescript
Solana	2020	Rust, C, C++
Polkadot	2020	Rust
Avalanche	2020	Go, Solidity, Typescript
NEAR	2020	Rust, Typescript
Internet Computer	2021	Rust, Modelica, Ocaml

Taulukko 3.3: 20 markkina-arvoltaan suurimman L1-protokollan julkaisuvuosi ja ensisijaiset ohjelmointikielet [64] [65].

Lohkoketjuprotokollien kehitysaktiivisuuteen vaikuttaa myös saatavilla oleva ammattitaito, joka ohjelmistokehityksessä on hyvin kieliriippuvaista. Slashdatan raportissa arvioidaan maailmassa olevan noin 31,1 miljoonaa ohjelmistokehittäjää, joista tällä hetkellä vain murto-osa hallitsee lohkoketjuteknologioiden kannalta oleellisia teknologioita. Taulukossa 3.4 on kuvattu eri ohjelmointikielten yhteisöjen kokoja.

Ohjelmointikieli	Ohjelmistokehittäjien lkm.
Javascript (sis. TypeScript, CoffeeScript)	17,4 M
Python	15,7 M
Java	14,0 M
C / C++	11,0 M
C#	10,0 M
PHP	7,9 M
Kotlin	5,0 M
Visuaaliset ohjelmointityökalut	5,0 M
Swift	3,5 M
Go	3,3 M
Objective C	2,4 M
Rust	2,4 M
Ruby	2,1 M
Dart	1,8 M
Lua	1,4 M
Solidity	0,2 M

Taulukko 3.4: Ohjelmointikieliyhteisöjen koot ja aktiiviset kehittäjät maailmanlaajuisesti Q1/2022. [66] [67]

3.4.3 Taloudelliset vaikuttimet

Koska kryptovaluutat ovat yksi lohkoketjujen merkittävimmistä sovelluksista, liittyy myös L1-lohkoketjujen vertailuun erottamattomasti monia taloudellisia elementtejä. Koska kullakin L1-lohkoketjulla on oma natiivirahakkeensa (engl. native token), kuten Bitcoin-lohkoketjun bitcoin tai Ethereumin ether, voidaan helposti verrata laskettujen rahakkeiden markkina-arvoa (engl. market cap). Markkina-arvolla tarkoitetaan rahakkeen markkinahintaa kerrottuna rahakkeiden määrällä. Markkina-arvon avulla voidaan voidaan arvioida erityisesti kryptovaluuttojen välistä suhteellista arvostusta.

Rahakkeiden arvostukseen liittyy myös rahakejakauma, jolla tarkoitetaan rahakkeiden omistuksen jakautumista eri tahoille. Merkittävää rahakkeiden keskittymistä voidaan pitää riskinä rahakkeen arvolle. Mikäli yksittäinen merkittävän osuuden rahakkeista omistava taho päättäisikin myydä osuutensa markkinoilla, olisi

sillä todennäköisesti merkittävä negatiivinen vaikutus rahakkeen markkina-arvoon. Työtodistus-lohkoketjujen rahakejakaumia pidetään yleensä reiluina, sillä rahakkeita vapautuu louhijoille keskimäärin louhintaan käytettyjen resurssien suhteessa. Ajoittain louhintaa on saatettu suorittaa jo ennen protokollan julkistamista nk. *esilouhintana* (engl. premine), jota ei pidetä tasapuolisena. Erityisesti Varantotodistejärjestelmää käyttävissä lohkoketjuissa on yleensä tilanne, jossa kaikki lohkoketjun rahakkeet on jo luotu ennen lohkoketjun käynnistämistä. Monet protokollat kuvaavat rahakkeidensa jakaumien periaatteita tokenomics-nimisessä dokumentissa, josta yleensä paljastuu miten suuri osuus rahakkeista on varattu esimerkiksi sijoittajille tai kehitystiimille ja millä aikataululla rahakkeita vapautuu markkinoille. Varantotodistuskonsesusta hyödyntävissä lohkoketjuissa rahakejakauma on myös merkittävä hajautukseen vaikuttava mittari, kuten osiossa 3.4. kuvataan.

Koska L1-lohkoketjut ovat käytännössä alustoja erilaisille älysopimuksiin perustuville sovelluksille, voidaan L1-lohkoketjuja arvottaa myös ekosysteemin *sovelluksiin kiinnitetyn arvon* (engl. total value locked, TVL) perusteella. Käytännössä korkea TVL kertoo kyseisen lohkoketjun varaan rakennettujen sovellusten käytön aktiivisuudesta ja arvostuksesta. Pääasiassa TVL muodostuu erityisesti *hajautettujen taloussovellusten* (engl. decentralized finance) eli DeFi-protokolliin sidotun valuutan yhteenlasketusta arvosta.

3.5 Lohkoketjun mainetekijät

Mainetekijöillä tässä tutkimuksessa tarkoitetaan erilaisia L1-protokolliin liittyviä ominaisuuksia, jotka eivät suoraan liity teknisiin tai käyttöön liittyviin ominaisuuksiin. Kyseessä on erityisesti mielikuviin vaikuttavista asioista.

L1-lohkoketjuprotokolliin liittyy erityisen paljon tulevaisuudenodotuksia. Merkittävä osa odotuksista kanavoituu kyseisten projektien nokkamiesten kautta. Perustajat ja pääkehittäjät ovat erityisasemassa määrittelemässä projektille visiota

ja muita strategisia tavoitteita, joten näille yksiläille annetaan paljon painoarvoa. Teknistä kyvykkyyttä arvostetaan merkittävästi ja tunnetuimpien protokollien keulahahmoina nähdäänkin monesti akateemikkoja tai esimerkiksi aikaisempien lohkoketjuprotokollien parissa meritoituneita hahmoja.

Kaikissa tapauksissa tietyn lohkoketjuprojektin perustajan henkilöllisyyttä ei tunneta. Tunnetuin esimerkki on Bitcoinin kehittänyt pseudonyymi Satoshi Nakamoto. Lohkoketjualalla yleisesti hyväksytään vielä kehittäjien anonyymiys tai nimimerkkien takaa toimiminen, joskin lisääntyneet määrät erilaisia petoksia ja huijauksia ovat tehneet kuluttajista ja sijoittajista varovaisempia ja epäileväisempiä. Anonyymiys nähdään kuitenkin toistaiseksi vielä neutraalina, ellei jopa positiivisena asiana.

Usein protokollan kehittäjät julkaisevat erilaisia teknisiä tiekarttoja (engl. roadmap) kuvaamaan kehityssuunnitelmia ja aiottua aikataulua. Näiden suunnitelmien toteumaa ja lupausten lunastamista seurataan tarkoin, eikä viivytyksiä katsota hyvällä, vaika ne alalla yleisiä ovatkin.

Lohkoketjuprotokollien arvostukseen vaikuttaa yleisesti merkittävästi, mikäli jokin tunnettu taho päättää sijoittaa protokollan kehitykseen tai sen rahakkeeseen. Lohkoketjut ja kryptovaluutat ovat suhteellisen tuore teknologian ja liiketoiminnan sektori, joten yleisesti tunnetut sijoittajat ja erityisesti institutionaaliset sijoittajat vahvistavat alan asemaa sijoituskohteena. Alalle erikoistuneet sijoitustoimijat voivat myös luoda tietyn protokollan rahakkeelle merkittävää kysyntää, suhteessa muihin protokolliin, sijoittamalla siihen.

Lohkoketjuteknologia ja kryptovaluutat on kehitetty internetin aikakaudella, joten internetkulttuuri on pesiytynyt syvälle alan ytimeen. Ajoittain tiettyjen protokollien ja valuuttojen suosion syynä on jonkinlainen vitsi tai meemi. Esimerkiksi yksi nykyisin markkina-arvoltaan suurimpia kryptovaluuttoja, dogecoin, on kehitetty vuonna 2013 parodiana kryptoalaa kohtaan. Dogecoinin suosiota on vaikea selittää

muulla kuin meemiarvolla.

4 Am I (really) here for the tech?

Tässä kappaleessa kuvataan tutkimuksessa käytetty tutkimusmenetelmä sekä käytetty tutkimusaineisto. Tutkimusaineiston osalta kuvataan sen koostumus sekä lähde. Luvussa kuvataan tulosten analysoinnissa käytettyjä menetelmiä sekä käytännön menetelmä, jolla tutkimus toteutettiin.

4.1 Tutkimusmenetelmä

Tämän tutkimuksen tavoitteena on selvittää mitä lohkoketjuekosysteemien ominaisuuksia lohkoketjuteknologian parissa toimivat ja kryptovaluuttoihin sijoittaneet yksilöt pitävät tärkeinä. Tutkimukselle muodostuivat seuraavat tutkimuskysymykset:

TK1: "Mitkä ensimmäisen asteen lohkoketjun ominaisuudet ovat tärkeimpiä?"

TK2: "Miten sijoittajanäkökulma eroaa kehittäjänäkökulmasta ominaisuuksia arvottaessa?"

TK3: "Onko kokemusvuosilla vaikutusta ominaisuuksien arvotukseen?"

TK4: "Onko suuremalla aktiivisuudella lohkoketju- ja virtuaalivaluuttateemojen parissa vaikutusta ominaisuuksien arvostukseen?"

Tämä tutkimus toteutettiin kvantitatiivisena eli määrällisenä tutkimuksena. Määrällisen tutkimuksen avulla voidaan tutkia esimerkiksi sosiaalisia ilmiöitä käyttäen tilastollista ja numeerista dataa [68]. Tutkimusaineisto kerättiin kyselytutkimuksen avulla. Kysely tutkimusmuotona sopii, kun tutkitaan ihmisten tietoutta tietystä ilmiöstä tai tilanteesta [69]. Kysely toteutettiin poikittaistutkimuksena, sillä se on

menetelmänä suoraviivainen ja tarvitsee toteuttaa vain kerran [68]. Kysely toteutettiin verkossa Google Forms -työkalun avulla ja siihen on kerättiin vastaajiksi lohkoketjuteknologioiden parissa toimineita ja kryptovaluuttoihin sijoittaneita yksilöitä. Kyselylomakkeen tulokset muokattiin paremmin luettavaan muotoon ja niitä analysoidaan regressioanalyysin ja kovarianssianalyysin avulla. Regressioanalyysi on tilastollinen työkalu, jolla voidaan tutkia ja löytää kausaalisuhteita muuttujien välillä [70]. Kovarianssianalyysilla eli yhteisvaihtelun analyysilla voidaan tutkia kahden muuttujan välistä korrelaatiota [71] ja se yhdistää regressio- ja varianssitutkimisen edut [72].

Tutkimuksen kyselyyn pyrittiin tavoittamaan vastaajiksi yksilöitä, jotka ovat toimineet lohkoketjuteknologian tai virtuaalivaluuttojen parissa riippumatta heidän kokemuksensa syvyydestä. Kyselyyn ei haluttu vastauksia yksilöiltä, joilla ei ollut aikaisempaa kosketusta alaan, sillä näitä vastauksia voitaisiin pitää sattumanvaraisina ja siten turhana kohinana vastauksia analysoidessa. Myös vastaajia, jotka olisivat täysin menettäneet mielenkiintonsa alaa kohtaan, pidettiin epätoivottavina.

4.2 Empiirinen vaihe ja käytännön toteutus

Kyselyn kysymykset luotiin pohjautuen aiempaan teoriatietoon ensimmäisen asteen lohkoketjuista. Kyselyn rakenne oli tarkoitus pitää mahdollisimman suoraviivaisena, jotta vastaaminen olisi nopeaa ja vaivatonta, eikä kyselyn vastaaminen jäisi aloittaneilta kesken. Kyselyssä oli yhteensä kahdeksan kysymystä, joissa annettiin kokonaisuudessaan 36 monivalintavastausta ja yksi avoin tekstivastaus. Kyselyn kysymykset oli jaettu kolmeen osioon, joista ensimmäinen osio keskittyi taustatietoihin, toinen osio L1-lohkoketjujen ominaisuuksien arvottamiseen ja kolmas osio vastausten validointiin tulevaisuuden arvioinnin avulla.

4.2.1 Taustatiedot

Ensimmäisessä osiossa tiedusteltiin kolmella kysymyksellä vastaajan taustoja suhteessa lohkoketjuteknologiaan ja kryptovaluuttoihin. Kyselyssä tiedusteltiin mikäli vastaaja piti ensisijaisesti itseään sijoittajana, kehittäjänä vai tasavahvasti molempina, vastaajan kokemusvuosia alan parissa sekä frekvenssiä alan kanssa tekemisissä olemisesta. Ensimmäisen osion kysymykset myös suunniteltiin yksinkertaisiksi ja helpoiksi, jotta ne toimisivat eräänlaisina lämmittelykysymyksinä vastaajille.

Kysymys 1.1: Käyttäjäpersoonat

Kysymyksessä 1.1 tiedusteltiin mihin käyttäjäpersoonaan vastaaja identifioi itsensä; sijoittajaan, kehittäjään vai molempiin. Kysymys on oleellinen TK2:en tutkimiseksi, sillä tarkoituksena on tutkia juuri sijoittajanäkökulman ja kehittäjänäkökulman omaavien henkilöiden eroja L1-ominaisuuksien arvostuksen suhteen. Kyseiset näkökulmat valikoituivat osaksi tutkimusta, sillä pääosa L1-lohkoketjuista on kehitetty avoimena lähdekoodina. Perinteisen näkemyksen mukaan avoimen lähdekoodin kehitysprojekteilla on kaksi sidosryhmää; ohjelmiston kehittäjä ja käyttäjä [73]. Tästä syystä myös L1-lohkoketjuilla voidaan karkeasti arvioida olevan kaksi erilaista sidosryhmää; (a) kehittäjät, jotka kehittävät L1-protokollia eteenpäin ja sovelluksia niiden päälle sekä (b) käyttäjät. L1-protokollien käytettävyys liittyy ensisijaisesti valuuttatransaktioiden välittämiseen ja toissijaisesti toimimiseen kehitysalustana älysopimuksille. L1-lohkoketjujen käyttäjien voidaan siis todeta käyttävän lohkoketjua joko virtuaalivaluutan vaihdantaan tai alustana sovellusten kehitykseen. Näistä käyttäjistä voidaan johtaa kyselyssä käytetyt käyttäjäpersoonat "sijoittaja"ja "kehittäjä"sekä heidän näkökulmansa.

Kysymys 1.2: Kokemusvuodet

Kysymyksessä 1.2. tiedusteltiin vastaajan kokemusvuosia lohkoketjuteknologian ja kryptovaluuttojen parissa. Kysymykseen vastattiin asteikolla 0—10, jossa 0=alle vuosi ja 10=kymmenen vuotta tai yli. Kysymys on oleellinen TK3:n tutkimiseksi, sillä tarkoitus on tutkia alan parissa toimimisen pituutta suhteessa vastaajien näkemyksiin. Lohkoketjuteknologia on verrattain uusi teknologian ala ja se on kasvanut hyvin nopeasti. Kyseiselle teknologiasektorille on kuitenkin ominaista syklisyys, jossa kiinnostus lohkoketjuteknologiaa ja kryptovaluuttoja kohtaan laskee julkisuudessa merkittävästi kasvaakseen taas myöhemmin eksponentiaalisesti. Sykli on toistaiseksi seurannut Bitcoin-lohkoketjun *puoliintumisen* (engl. halving) neljän vuoden sykliä. Tarkoituksena on tutkia, mikäli useamman neljän vuoden syklin nähneet veteraanit arvostavat eri asioita, kuin tuoreemmat uudet tulokkaat.

Kysymys 1.3: Aktiivisuus aiheen parissa

Kysymyksessä 1.3 tiedusteltiin kuinka usein vastaaja on tekemisissä lohkoketju- tai kryptovaluutta-aiheiden kanssa. Kysymykseen vastattiin nominaaliasteikolla, jossa vastauskategoriat olivat "päivittäin", "viikoittain", ja "kuukausittain". Kysymys on oleellinen TK4:n tutkimiseksi, sillä ala kehittyy nopeasti ja sille syntyy jatkuvasti uudenlaisia teknologiakäsitteitä sekä liiketoimintakonsepteja. Tarkoituksena on tutkia, mikäli harvemmin alan parissa toimivat arvostavat eri asioita, kuin aktiivisemmin kehitystä seuraavat.

4.2.2 L1-lohkoketjujen ominaisuuksien arvottaminen

Kyselyn toisessa osiossa tiedusteltiin vastaajan näkemyksiä erilaisten lohkoketjujen teknisten, käyttöön liittyvien ja maineeseen liittyvien ominaisuuksien arvostamisen suhteen. Kysymykset oli aseteltu siten, että vastaaja valitsi kunkin 32 eritellyn ominaisuuden osalta erikseen, miten merkittävänä lohkoketjun ominaisuutena tätä piti.

Vastaaminen tehtiin viisiportaisella nominaaliasteikolla, jossa 1 = ei lainkaan merkitystä ja 5 = kriittinen merkitys. Osion kysymykset ovat oleellisia päätutkimuskysymyksen TK1:n tutkimiseksi. Kuhunkin kysymykseen on pyritty valikoimaan L1-lohkoketjuille eri tavoin merkityksellisinä pidettäviä ominaisuuksia, joskin ne on pyritty esittämään vastaajalle neutraalisti ja samanarvoisina. Ominaisuuksia on käsitelty tarkemmin tutkimuksen pääluvussa 3.

Kysymys 2.1: Tekniset ominaisuudet

Kysymys 2.1 liittyi L1-lohkoketjujen teknisiin ominaisuuksiin. Vastaajaa pyydettiin arvioimaan miten tärkeinä ominaisuuksina hän pitää käytettyä konsensusmekanismia, aktiivisten noodien lukumäärää, noodin ylläpitämisen alhaisia vaatimuksia, transaktioiden varmennusaikaa, lohkokokoa, transaktiokuluja, transaktionopeutta, transaktioiden kokonaiskapasiteettia, kolmannen osapuolen L2-skaalausratkaisujen olemassaoloa, ohjelmointikieltä ja transaktioiden obfuskointia. Listatut ominaisuudet olivat tunnettuja eri L1-lohkoketjuja toisistaan erottavia teknisiä tekijöitä, jotka liittyivät lohkoketjutrilemman kolmen pääkohdan, eli skaalautuvuuden, hajautuksen ja turvallisuuden rakenneosiin. Vastaukset antoivat viitteitä siitä, miten vastaaja yleisesti arvostaa itse lohkoketjuteknologian kehitystä ja sen taustaperiaatteita.

Kysymys 2.2: Käyttöön liittyvät ominaisuudet

Kysymys 2.2 liittyi L1-lohkoketjujen käyttöön liittyviin ominaisuuksiin. Vastaajaa pyydettiin arvioimaan miten tärkeinä ominaisuuksina hän pitää yhteisön aktiivisuustasoa, L1-lohkoketjun päälle rakennettujen projektien ja hajautettujen sovellusten määrää, käyttäjien ja lompakoiden määrää, transaktioiden kokonaisvolyymiä, ohjelmistokehitysaktiivisuutta, natiivin rahakkeen markkina-arvoa, *L1-lohkoketjuun sidottua kokonaisarvoa* (engl. total value locked, TVL), natiivin rahakkeen arvoa, rahakkeen inflaatiotasoa, rahakkeen vaihdannan volyymiä, aktiivisen NFT-ekosysteemin

olemassaoloa ja aktiivisen GameFi-ekosysteemin olemassaoloa. Listatut ominaisuudet ovat tunnettuja eri L1-lohkoketjuja toisistaan erottavia tekijöitä, jotka liittyvät erityisesti L1-lohkoketjun päälle rakentuneen ekosysteemin aktiivisuuteen ja toimintaan, sekä L1-lohkoketjulle ominaisen natiivin valuutan vaihdantaan. Vastaukset antoivat viitteitä siitä, miten vastaaja itse hyödyntää lohkoketjuteknologiaa.

Kysymys 2.3: Maineeseen liittyvät ominaisuudet

Kysymys 2.3 liittyi L1-lohkoketjujen maineeseen liittyviin ominaisuuksiin. Vastaajaa pyydettiin arvioimaan miten tärkeinä ominaisuuksina hän pitää *rahakejakaumaa* (engl. tokenomics), institutionaalisten sijoittajien olemassaoloa, nk. julkkissijoittajien olemassaoloa, nk. meemiarvoa, tietoa projektin perustajan henkilöllisyydestä, projektin perustajan maineesta, tuotekehityksen välitavoitteiden saavuttamista, historiaa tietoturvamurroista tai muista -haasteista ja *ensimmäisen toimijan etua* (engl. first mover advantage). Listatut ominaisuudet ovat tunnettuja eri L1-lohkoketjuja toisistaan erottavia mainetekijöitä, jotka liittyvät ekosysteemeihin pääosin välillisesti. Lohkoketjuhankkeita voi monella tapaa verrata startup-yrityksiin, joihin sijoittajat ja kehittäjät käyttävät resurssejaan tulevaisuudessa palautuvan tuoton vuoksi. Eri markkinatoimijoiden luotto tai luottamuksen menetys voi osoittautua myös L1-protokollien menestyksen määrittäjäksi. Vastaukset antoivat viitteitä siitä, minkä tekijöiden varaan vastaaja rakentaa mahdollisen luottamuksen ja tulevaisuudenuskon.

4.2.3 Tulevaisuuden arviointi

Kyselyn kolmannessa osiossa selvitettiin vastaajan arviota tulevaisuuden kehityksestä kahdella kysymyksellä. Vastaajilta tiedusteltiin monivalintakysymyksellä todennäköisimmin menestyviä L1-lohkoketjuekosysteemejä sekä avoimella tekstikysymyksellä parhaiten taloudellisesti menestyvää L1-lohkoketjulle natiivia kryptovaluuttaa.

Kysymys ei suoraan vastaa mihinkään tutkimuskysymykseen, mutta voi välillisesti vahvistaa tai kumota aikaisemmin annettuja vastauksia. Vastauksia käsiteltiin lähinnä arvauksina, joina vastaajatkin varmasti vastauksiaan pitivät.

Kysymys 3.1: Menestyvät L1-ekosysteemit

Kysymys 3.1 oli monivalintakysymys, jossa vastaajaa pyydettiin valitsemaan 26 listatun joukosta 1—4 L1-lohkoketjuekosysteemiä, jolla vastaaja koki olevan parhaat edellytykset menestykseen tulevaisuudessa. Listaan oli pääosin valittu Coinmarketcap.com -verkkosivuston listauksesta L1-protokollat, joiden natiivirahakkeiden markkina-arvo ylsi 100 suurimman virtuaalivaluutan markkina-arvon joukkoon ennen kyselyn lähettämistä. Vastausvaihtoehtona oli myös "muu", sillä tarkoitus ei ollut johdatella vastaajaa ja rajoittaa vastauksia, vaan tehdä sekä vastaamisesta että vastausten analysoinnista mahdollisimman suoraviivaista.

Kysymys 3.2: Virtuaalivaluutta, jolla paras viiden vuoden hintakehitys

Kysymys 3.2 oli avoin tekstikysymys, jossa vastaajaa pyydettiin kirjaamaan L1-lohkoketjun natiivirahake, jolla uskoo olevan paras hintakehitys viiden vuoden aikajänteellä. Toisin kuin kysymyksessä 3.1, keskityttiin tässä ekosysteemikehityksen sijaan vain yksittäisen virtuaalivaluutan arvoon. Tämä on merkityksellistä lähinnä siksi, että kysymyksenasettelu mahdollistaa helpommin myös vanhempien sukupolven L1-protokollien, joilla ei ole aktiivista ekosysteemikehitystä, mahdollisen valinnan. Kysymys oli avoin tekstikysymys, jotta vastaajia johdateltaisiin mahdollisimman vähän. Tutkimusta tehdessä vastauksia arvioitiin tulevan maltillinen määrä, jotta avoimen tekstivastauksen käsittely ei osoittautuisi liian työlääksi.

4.2.4 Kyselyyn vastaajien valinta

Kyselyn vastaajia pyrittiin keräämään lähinnä sosiaalisen median avulla. Kyselyn verkkolomakkeelle vievää linkkiä jaettiin avoimesti kirjoittajan LinkedIn- ja Twitter-profiilien päivityksissä, työyhteisön Slack-kanavalla sekä kolmen eri lohkoketjuprotokollan kehitys- ja käyttäjäyhteisön Discord-kanavalla. LinkedIn-päivitys oli 23.06.2022 mennessä tavoittanut 1228 henkilöä ja kaksi Twitter-päivitystä olivat tavoittaneet 66 ja 76 henkilöä. Työyhteisön Slack-kanavalle lähetetty viesti oli arviolta tavoittanut noin 20 henkilöä. Kolmella lohkoketjuteemaisella Discord-palvelimella, joille kyselylinkki jaettiin, oli yhteensä noin 40000 jäsentä.

Discord-palvelun luonteen vuoksi oli todennäköistä, että kyselylinkki ei tavoittanut suurinta osaa palvelimien jäsenistä. Merkittävä osa jäsenistä lohkoketjuprotokollan kehitys- ja käyttäjäyhteisöjen palvelimilla ovat yleisen kokemuksen mukaan hyvin passiivisia osallistujia. Krypto-teemaisiin yhteisöihin on myös pesiytynyt epäluulo erilaisia ehdotuksia ja linkkejä kohtaan, sillä moninaiset huijaukset ovat yleisiä. Suurin osa kyselyn vastaajista tavoitettiin tedonnäköisesti LinkedInin ja työyhteisön Slack-kanavan kautta, sillä näissä kanavissa vastaajilla on todennäköisimmin ollut jonkinlainen henkilökohtainen suhde kyselyn tekijään ja siten alhaisempi kynnys osallistua. Kyselyyn vastasi yhteensä 33 henkilöä.

4.3 Kyselyn tulokset

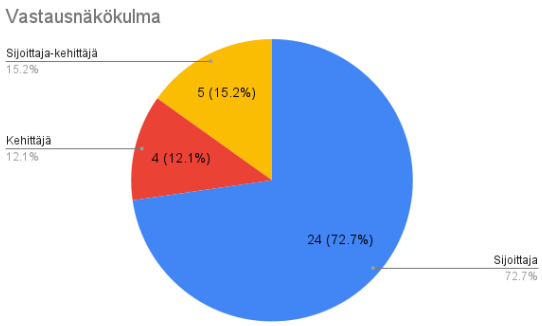
Kyselyyn vastasi yhteensä 33 vastaajaa. Kyselyn tuloksia analysoitiin regressioanalyysilla jakamalla vastaajat taustatietokysymysten mukaisesti eri vertailuryhmiin ja vertailemalla eri ryhmien keskimääräisiä vastauksia. Taustatietoihin liittyvät vastaukset annettiin nominaaliasteikoilla. Lohkoketjujen ominaisuuksien arvostamiseen liittyvät vastaukset annettiin kyselyssä suhdeasteikolla 1—5, jossa 1 = ei lainkaan merkitystä ja 5 = kriittinen merkitys. Tulosten analysoimisen helpottamiseksi tulok-

sia tulkittiin suhdeasteikolla 0—4, jossa 0 = ei lainkaan merkitystä ja 4 = kriittinen merkitys. Tulevaisuuden arviointiin liittyvät vastaukset annettiin avoimina monivalintavastauksina ja avoimina tekstivastauksina, joita käytännössä analysoitiin nominaaliasteikkona.

Tutkimuksen tilastollinen merkitsevyys vaihtelee, sillä tilastollisen merkitsevyyden rajana pidetään yleisesti minimissään 30 otoksen joukkoa. Vaikka kyselyyn vastasi 33 henkilöä, on merkittävä osa tulosten analysoinnista keksittynyt vertailemaan vastaajajoukon pienempiä osajoukkoja, eli vertailuryhmiä. Vertailuryhmiä tarkastellessa tuloksia ei voida pitää tilastollisesti merkitsevinä, vaan enemmänkin suuntaa antavina.

4.3.1 Taustatietojen analysointi

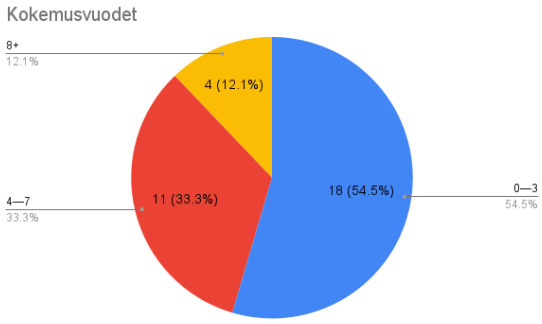
Kyselyyn vastanneista suurin osa (72%) kategorisoi itsensä ensisijaisesti sijoittaja -luokkaan. 12,17% vastaajista kategorisoi itsensä ensisijaisesti kehittäjiksi ja 15,9% piti itseään tasapuolisesti molempiin ryhmiin kuuluvana. Vastausten jakauma oli odotuksien mukainen, sillä yleisesti sovelluksien käyttäjiä on kehittäjiä enemmän.



Kuva 4.1: Vastaajien näkökulmajakauma

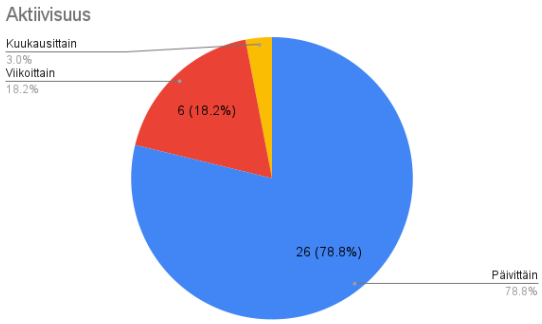
Kyselyyn vastanneista suurin osa (72,7%) on tutustunut kryptovaluuttoihin ja lohkoketjuteknologiaan kuluneen kolmen vuoden aikana, eli vuosina 2022—2020. Vähintään neljä ja enintään seitsemän vuotta kryptojen parissa toimineita oli kolmannes (33,3 %) vastaajista. Kahdeksan vuotta tai enemmän kryptojen parissa oli viettänyt 12,1% vastaajista. Vastausluokat ovat siinä mielessä havainnollisia, että 0—3 vuotta markkinassa olleet ovat kohdanneet

enintään yhden markkinasyklin, 4—7 vuotta mukana olleet ovat kohdanneet enintään kaksi ja sitä pitempään mukana olleet jo kolme. Vastausten jakauma oli odotuksien mukainen, sillä ala on teknologia-alana suhteellisen uusi, mutta on kasvanut vuosien kuluessa eksponentiaalisesti. Näin on ilmeistä, että uusia ihmisiä päätyy kryptoalan pariin kiihtyvää tahtia.



Kuva 4.2: Vastaajien kokemusvuosijakauma

Kyselyyn vastanneista suurin osa (78,8%) on päivittäin tekemisissä kryptovaluuttojen ja lohkoketjuteknologian kanssa. 18,2% kertoi olevansa tekemisissä kryptojen kanssa viikoittain ja yksi vastaaja (3%) kuukausittain. Vastausten jakauma oli odotuksien mukainen, sillä aktiivinen toiminta nopeasti kehittyvällä ja muuttuvalla teknologiasektorilla vaatii aktiivista perehtymistä. Toisaalta kryptoalasta on uutisoitu paljon ja toimijat tuottavat jatkuvasti enemmän materiaalia tavoittamaan uusia tahoja, joten aiheeseen saatta törmätä helposti, vaikka ei eritysesti sitä seuraisikaan.



Kuva 4.3: Vastaajien aktiivisuusjakauma

4.3.2 Erot arvostuksessa

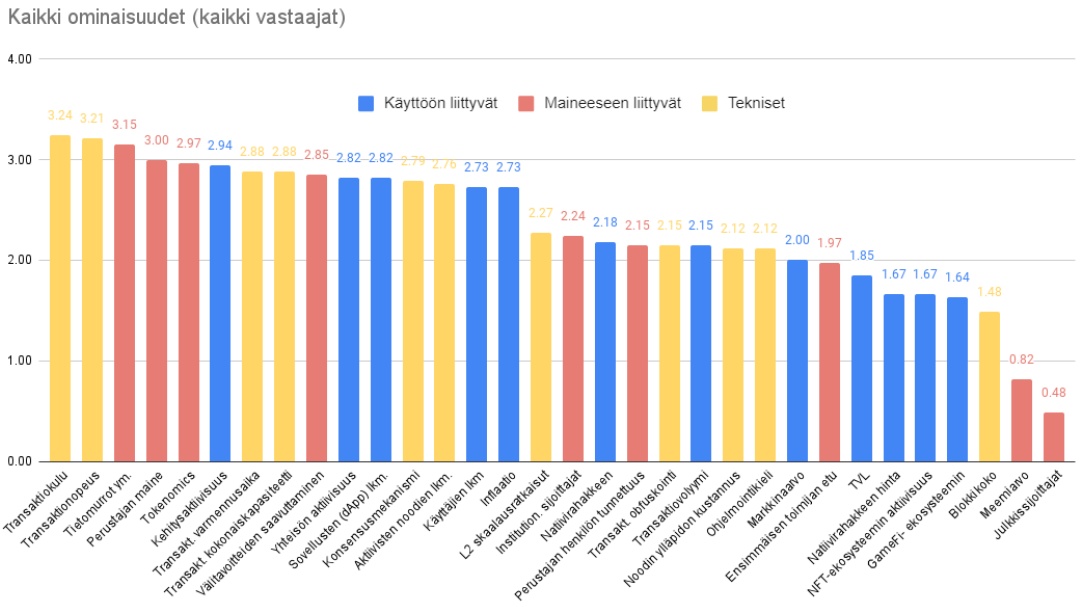
Kyselyssä oli listattu 33 eri L1-lohkoketjun ominaisuutta, joiden arvostusta tutkittiin. Lohkoketjujen ominaisuuksien arvostamiseen liittyvät vastaukset annettiin kyselyssä suhdeasteikolla 1—5, jossa 1 = ei lainkaan merkitystä ja 5 = kriittinen merkitys. Tulosten analysoimisen helpottamiseksi tuloksia tulkittiin suhdeasteikolla 0—4, jossa 0 = ei lainkaan merkitystä ja 4 = kriittinen merkitys. Käytännössä tuloksissa tarkasteltiin pistevaihteluvälejä, joissa 3—4 = tärkein pisteneljännes, 2—3 = toiseksi tärkein, 1—2 kolmanneksi tärkein ja 0-1 neljänneksi tärkein eli vähiten tärkeä pisteneljännes.

Ominaisuudet oli jaettu karkeasti kolmeen kategoriaan: (a) teknisiin ominaisuuksiin, (b) käyttöön liittyviin ominaisuuksiin ja (c) maineeseen liittyviin ominaisuuksiin. Vastaajien vertailuryhmiä oli yhteensä yhdeksän. Eroja ominaisuuksien arvostamisessa vertailtiin vertailuryhmien sekä ominaisuuskategorioiden välillä.

Koko vastaajajoukko

TK1:een vastaamiseksi tarkasteltiin erityisesti tärkeintä pisteneljännestä. Koko vastaajajoukkoa tarkastellessa kaikista tärkeimmässä pisteneljänneksessä olivat transaktiokulujen suuruus (3,24), transaktionopeus (3,21), lohkoketjun turvallisuusongelmat (3,15) ja lohkoketjuprojektin perustajan maine (3,0). Tuloksissa korostuvat ominaisuudet, jotka suoraan vaikuttavat kryptosovellusten käyttöön. Näitä olivat käyttökustannukset ja transaktionopeus, jonka yleisesti oletetaan vaikuttavan eri palveluiden toiminnallisuuksien kehitysmahdollisuuksiin. Samaten korostuivat voimakkaasti turvallisuusteemat, sillä tietoa projektien ja protokollien turvallisuusongelmista ja menneisyyden haasteista arvostettiin. Myös projektin perustajan maine kiinnosti, sillä pääosa L1-protokollista on edelleen tuotekehityksessä. Perustajan aiemmat saavutukset tai luurangot kaapissa vaikuttavat väistämättä odotuksiin luotsatun projektin suhteen. Vähiten tärkeään pisteneljännekseen pisteytettiin lohko-

ketjun meemiarvo (0,82) ja tieto julkisuuden henkilöiden sijoittamisesta kyseiseen lohkoketjuun (0,48).



Kuva 4.4: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso

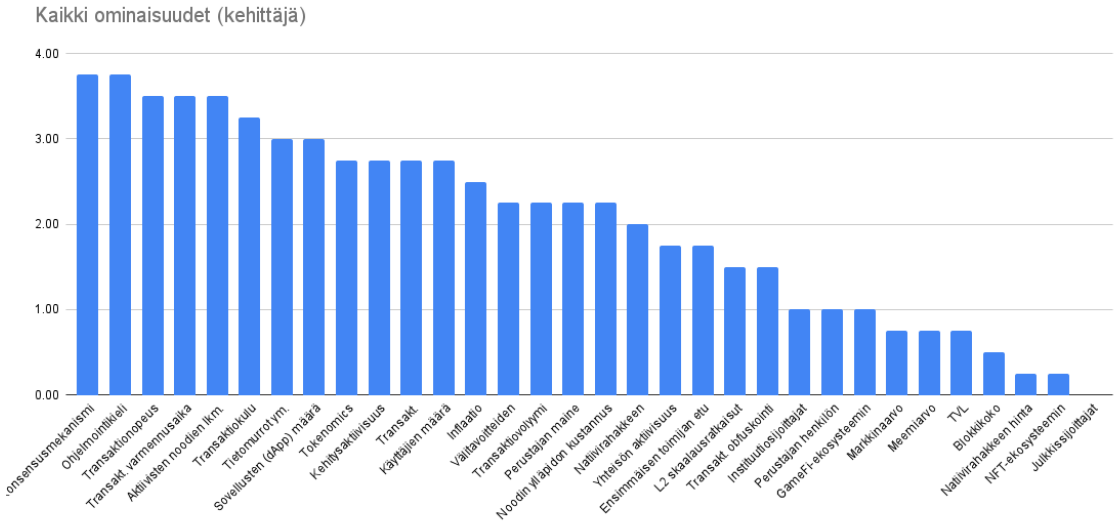
Kaikkien vastaajien osalta eri ominaisuuksien arvottamisessa oli suhteellisen paljon vaihtelua, sillä eri ominaisuuksien vastausten keskimääräinen keskihajonta oli 1,07. Suurin keskihajonta vastauksissa ja siten suurin vaihtelu vastaajien näkemyksissä koski projektin perustajan henkilöllisyyden tuntemista (1,50). Tulos oli odotettu, sillä alalla toimivien suhteelliseen anonyymiyteen suhtaudutaan hyvin kaksijakoisesti. Vastaavasti alhaisin keskihajonta ja siten suurin yhtenäisyys vastauksissa koski lohkoketjujen turvallisuusongelmien merkitystä (0,76).

Koko joukkoa tarkastellessa ominaisuuskategoriat erosivat toisistaan siten, että teknisiä ominaisuuksia pidettiin keskimäärin merkityksellisimpinä vastauskeskiarvolla 2,54. Seuraavaksi merkityksellisin kategoria oli käyttöön liittyvät ominaisuudet vastauskeskiarvolla 2,27 ja kolmantena maineeseen liittyvät ominaisuudet vastaus-

keskiarvolla 2,18. Kategoriavertailua voidaan kuitenkin pitää lähinnä viitteellisenä mittarina, sillä kyselyssä mainittuja ominaisuuksia ei voida pitää kattavana listauksena kategorioiden ominaisuuksista. Ei voida siis sulkea pois vaihtoehtoa, jossa tiettyyn kategoriaan tulkittava, mutta kyselystä puuttuva ominaisuus, olisi kyselyssä mukana ollessaan merkittävästi muuttanut vastauskeskiarvoja. Tulokset kuitenkin olivat odotusten mukaisia, sillä kryptoala on hyvin tekninen ja se antaa toistaiseksi vielä rajallisesti mahdollisuuksia osallistua ilman hyvää uuden teknologian omaksumiskykyä.

Kehittäjät

Kun tarkasteltiin kehittäjä-vertailuryhmän vastauksia, korostuivat kyselyssä odotetusti L1-lohkoketjujen tekniset ominaisuudet. Teknisten ominaisuuksien pistekeskiarvo oli 2,70, käyttöön liittyvien ominaisuuksien pistekeskiarvo 1,67 ja maineeseen liittyvien ominaisuuksien 1,64.



Kuva 4.5: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso kehittäjien keskuudessa

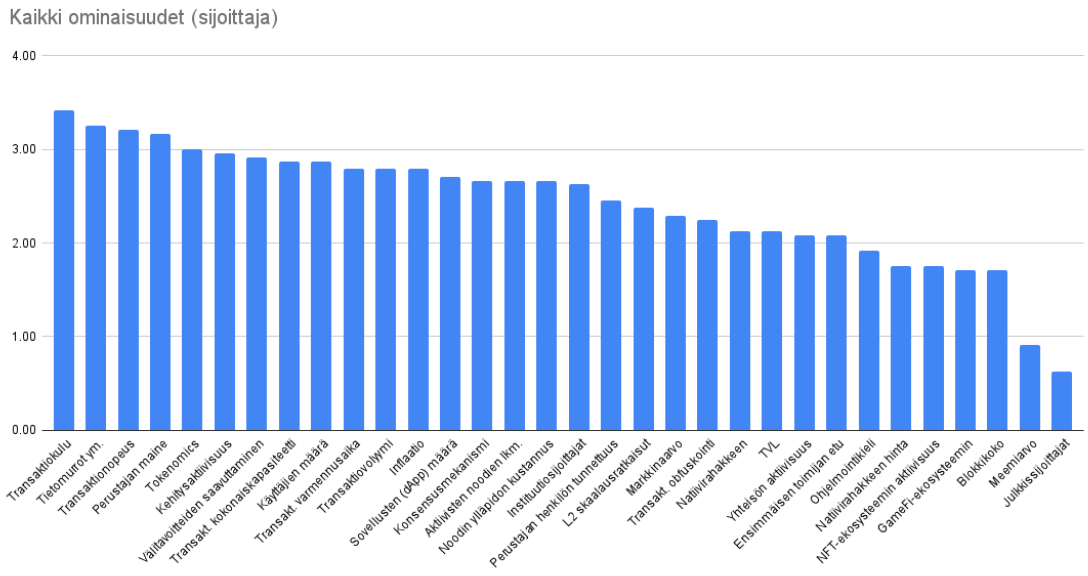
Tärkeimpään pistevaihteluneljännekseen nousivat lohkoketjun konsensusmekanismi (3,75), ohjelmointikieli (3,75), transaktionopeus (3,50), transaktioiden varmennusaika (3,50), aktiivisten noodien lukumäärä (3,50), transaktiokulut (3,25), turvallisuusongelmat (3,00) sekä hajautettujen sovellusten lukumäärä (3,00). Kehittäjiä siis kiinnostivat ensisijaisesti suoraan L1-protokollien parissa tehtävään ohjelmistokehitykseen vaikuttavat asiat. Myös hajautettujen sovellusten lukumäärä kiinnosti, sillä se välillisesti viestii L1-lohkoketjun ekosysteemin suosiosta ja elinvoimasta. Tällä voi olla suora vaikutus esimerkiksi kehitystyön tulevaan kysyntään kyseisen protokollan teknologioiden parissa.

Kehittäjät olivat hyvin yksimielisiä julkkissijoittajien merkityksettömyydestä, sillä vastausten keskiarvo ja keskihajonta oli 0. Tulos ei ole yllättävä, sillä julkkissijoittajat sekä myös meemiarvo (vastauskeskiarvo 0,75) liittyvät pääasiassa markkinointiteemoihin, joilla ei ole suoraa liittymäkohtaa tuotekehitykseen. Hyvin alhaisen merkityksen ominaisuuksia olivat myös natiivirahakkeen hinta (0,25) ja NFT-ekosysteemin aktiivisuus (0,25). Alhaisimmat vastausten keskihajonnat olivat juuri tärkeimpinä ja merkityksettömimpinä pidetyillä ominaisuuksilla. Suurin keskihajonta ja siten isoimmat näkemyserot liittyivät yhteisön aktiivisuuden arvostukseen (2,06).

Sijoittajat

Sijoittajien keskuudessa tärkeimpään pistevaihteluneljänneksessä olevat ominaisuudet olivat transaktiokulut (3,42), turvallisuusongelmat (3,25), transaktionopeus (3,21), perustajan maine (3,17) ja rahakejakauma (3,00). Yhteistä ominaisuuksille on, että ne ovat kaikki edellytyksiä L1-protokollan käytön yleistymiselle ja käyttäjien lisääntymiselle tulevaisuudessa. Sijoittajien mielestä vähiten merkityksellisiä tekijöitä olivat julkkissijoittajat (0,63) ja meemiarvo (0,92). Alhaisin keskihajonta liittyi turvallisuusongelmien arvostukseen (0,68) ja suurin koski projektin perustajan henkilöl-

lisyyden tuntemista (1,50). Tulokset ovat hyvin samankaltaisia, kuin koko vastausjoukkoa tarkastellessa, sillä sijoittajat muodostavat selkeästi suurimman yksittäisen vertailuryhmän 72% osuudella vastaajista.

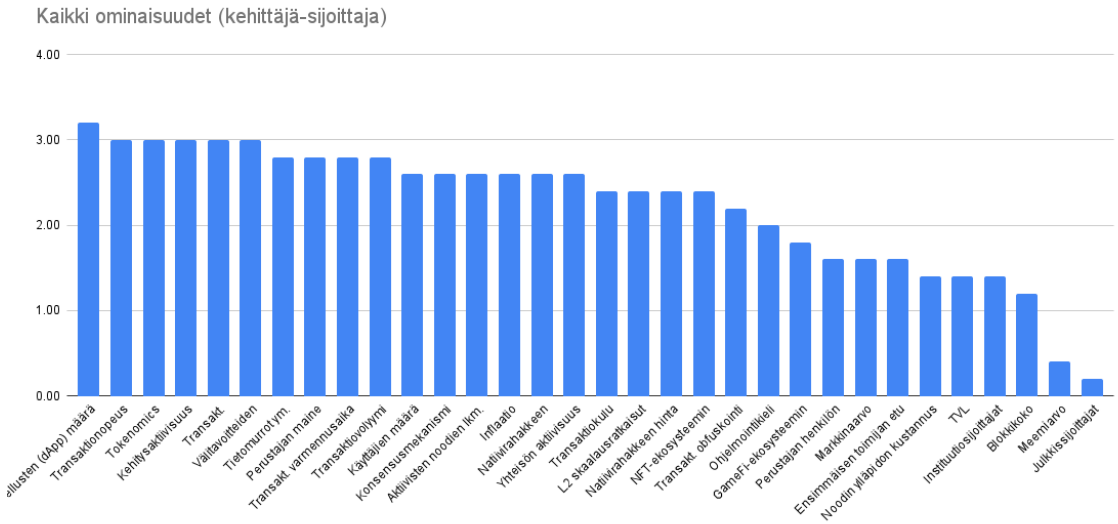


Kuva 4.6: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso sijoittajien keskuudessa

Kehittäjä-sijoittajat

Kehittäjä-sijoittajien vastauksissa korostui muutama ominaisuus, joita ei ollut kehittäjien tai sijoittajien arvostetuimpien ominaisuuksien listalla. Näitä olivat kehitysaktiivisuus (3,00), transaktioiden kokonaiskapasiteetti (3,00) ja välitavoitteiden saavuttaminen (3,00). Nämä sekä tärkeimpänä pidetty hajautettujen sovellusten lukumäärä (3,20) liittyvät erityisesti L1-lohkoketjujen ekosysteemikehitykseen pidemmällä aikavälillä. Kehittäjä-sijoittajilla tuntuu olevan laaja-alaisin katsantokulma lohkoketjujen ominaisuuksien arvostamiseen. Muitan ominaisuuksia tärkeimmässä pisteneljänneksessä olivat transaktionopeus (3,00) ja rahakejakauma (3,00).

Suurin keskihajonta liittyi erityisesti konsensusmekanismin arvostukseen (1,67), mikä oli jokseenkin yllättävää. Konsensusmekanismi itsessäänhän on välttämätön osa lohkoketjujärjestelmää. Osalle vastaajista tietynlainen konsensusmekanismi on selvästi kriittinen palanen L1-lohkoketjun tulevaisuutta ja osalle se tuntuu olevan "vain"tekninen haaste, joka ratkeaa tavalla tai toisella. Pienin keskihajonta liittyi julkkissijoittajiin (0,45), sillä myös kehittäjä-sijoittajat olivat melkein yksimielisiä niiden merkityksettömyydestä.



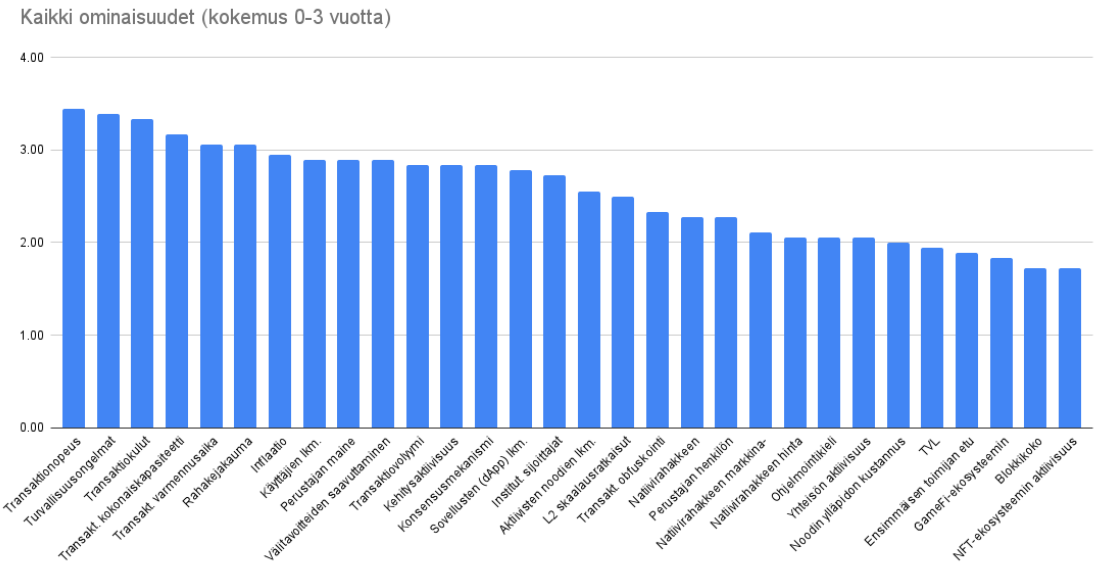
Kuva 4.7: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso kehittäjä-sijoittajien keskuudessa

0—3 vuotta kokemusta omaavat

Alle neljä vuotta kokemusta kryptoalasta omaavilla tärkeimmäksi ominaisuudeksi nousi L1-lohkoketjun transaktionopeus keskiarvolla 3,44 ja keskihajonnalla 0,70. Muut tärkeimpään pisteneljännekseen yltäneet ominaisuudet olivat turvallisuusongelmat (3,39), transaktiokulut (3,33), transaktioiden kokonaiskapasiteetti (3,17), transaktioiden varmennusaika (3,06) ja rahakejakauma (3,06). Kärkiominaisuuksien

arvostus oli hyvin yhtenäistä pienellä keskihajonnalla (0,70—0,94). Vähiten arvostustettiin jälleen julkkissijoittajia (0,50) ja meemiarvoa (0,78), joskin keskihajonta oli julkkissijoittajien osalta hieman suurempi, kuin muissa vertailuryhmissä (1,04).

Selkeä enemmistö (77,78%) vastaajista kuului myös sijoittajat -vertailuryhmään, joten sijoittajien vastaukset painottuivat vastauksissa. Molemmilla ryhmillä oli samat kolme ominaisuutta kolmen arvostetuimman joukossa, joskin hieman eri järjestyksessä. Kehittäjiin ja kehittäjä-sijoittajiin kuului molempiin 11,11% vertailuryhmän vastaajista.



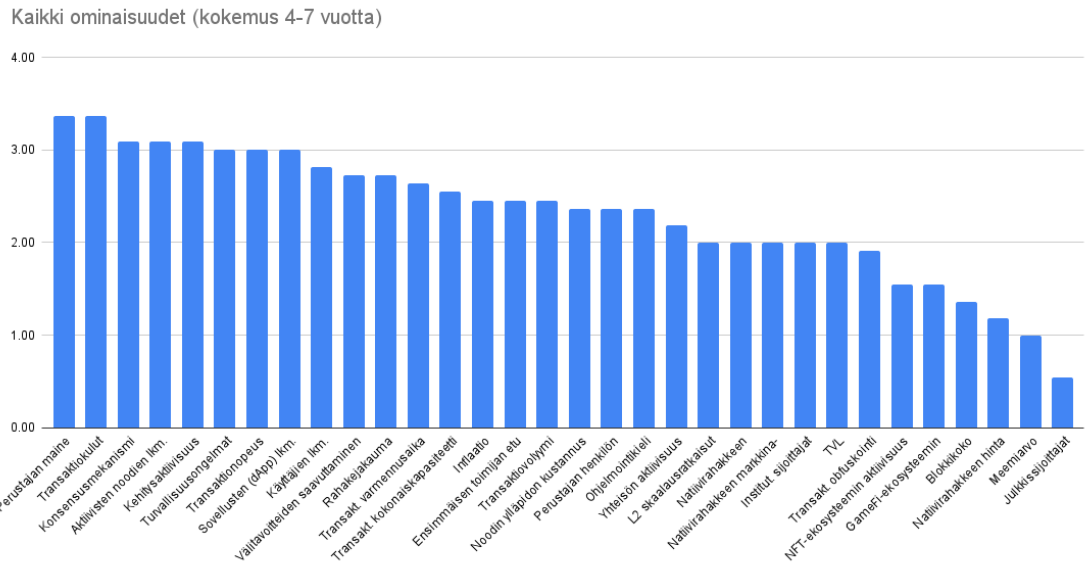
Kuva 4.8: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso 0—3 vuotta kokemusta omaavien keskuudessa

4—7 vuotta kokemusta omaavat

Jo edellisen kryptosyklin aikana (2015—2018) alalla mukana olleet vastaajat pitivät keskimäärin perustajan mainetta (3,36) ja transaktiokuluja (3,36) tärkeimpinä L1-ominaisuuksina. Konsensusmekanismia, aktiivisten noodien lukumäärää ja eko-

systeemin kehitysaktiivisuutta arvostettiin jaetun kolmannen sijan arvoisesti (3,09). Loput tärkeimmässä pisteneljänneksessä olevat ominaisuudet olivat turvallisuusongelmat, transaktionopeus ja hajautettujen sovellusten lukumäärä pistekeskiarvolla 3,00. Heikoimmin arvostettuja ominaisuuksia olivat julkkissijoittajat (0,55) ja meemiarvo (1,00). Meemiarvolla nähtiin vastaajien joukossa tosin myös arvoa, sillä keskihajonta oli muita vertailuryhmiä suurempi (1,34).

Enemmistö kokemusvälille sijoittuvista vastaajista (72,7%) kuului sijoittaja-vertailuryhmään Kehittäjiä oli 18,2 ja kehittäjä-sijoittajia 9,1% vastaajista.

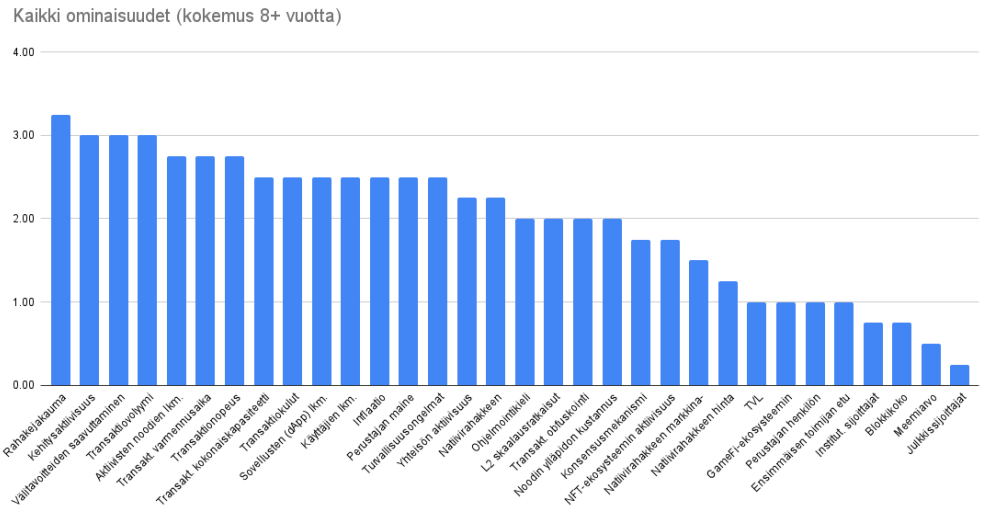


Kuva 4.9: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso 4—7 vuotta kokemusta omaavien keskuudessa

8+ vuotta kokemusta omaavat

Yli kahdeksan vuotta kryptoalan kanssa tekemisissä olevat vastaajat arvostivat eniten rahakejakaumaa (3,25), kehitysaktiivisuutta (3,00), välitavoitteiden saavuttamista (3,00) ja transaktiovolyymia (3,00). Mainitut ovat kaikki lohkoketjun käyt-

töön tai toteutuneeseen toimintaan liittyviä ominaisuuksia. Vaikka pääosa teknisistä ominaisuuksista nousee kyllä kolmanteen pisteneljännekseen, vastauksista saa sen vaikutelman, että alan veteraanit ovat kiinnustuneita konkreettisesta toiminnasta ja reaalituloksista. Samaa voidaan päätellä myös hajanaisista vastauksista liittyen perustajan maineeseen, sillä korkea keskihajonta (1,91) kertoo osan vastaajista pitävän ominaisuutta tärkeänä ja osa merkityksettömänä. Ylipäätään pisimmän kryptokokemuksen omaavat antoivat varautuneimmin pisteitä ominaisuuksille. Vertailuryhmä antoi keskimäärin pisteet 1,97, kun taas vertailuryhmä 0—3 kokemusvuotta antoi keskimäärin pisteet 2,43 ja vertailuryhmä 4—7 kokemusvuotta pisteet 2,32. Vastausten perusteella kokemusvuodet tuovat mukanaan kriittisyyttä, minkä avulla voi karsia "turhaa kohinaa". Muiden ryhmien tapaan heikoimmat pisteet saivat julkkissijoittajat (0,25) ja meemiarvo (0,50). 50% vertailuryhmän vastaajista oli sijoittajia ja 50% kehittäjä-sijoittajia.

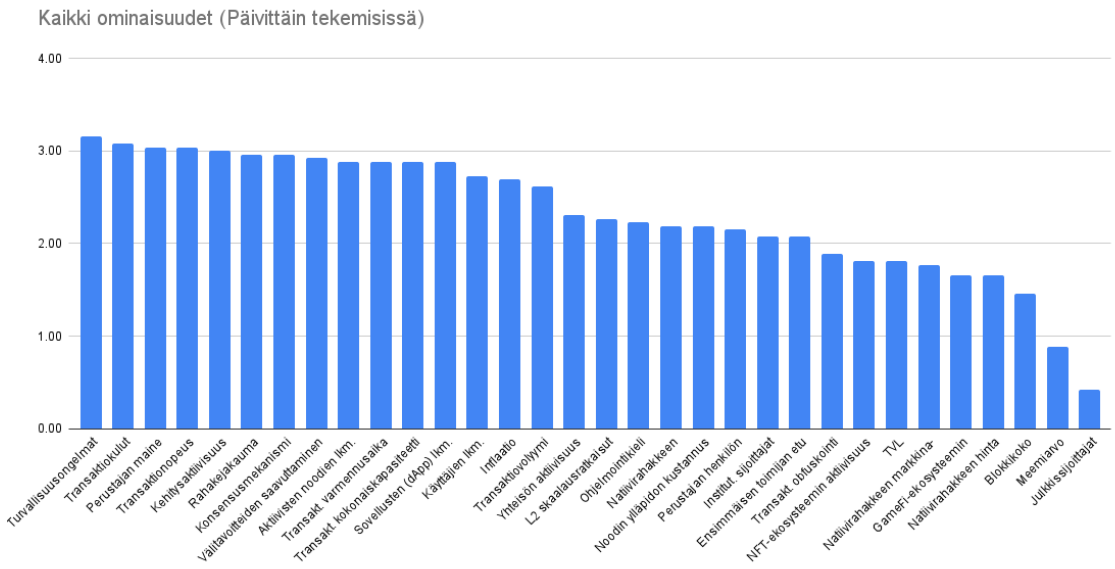


Kuva 4.10: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso yli 8 vuotta kokemusta omaavien keskuudessa

Aktiivisuus

Sillä kuinka usein henkilö on tekemisissä kryptojen kanssa tuntui olevan vaikutusta arvostettuihin ominaisuuksiin, joskin ilmiön syistä oli kerätyllä datalla haastava tehdä johtopäätöksiä.

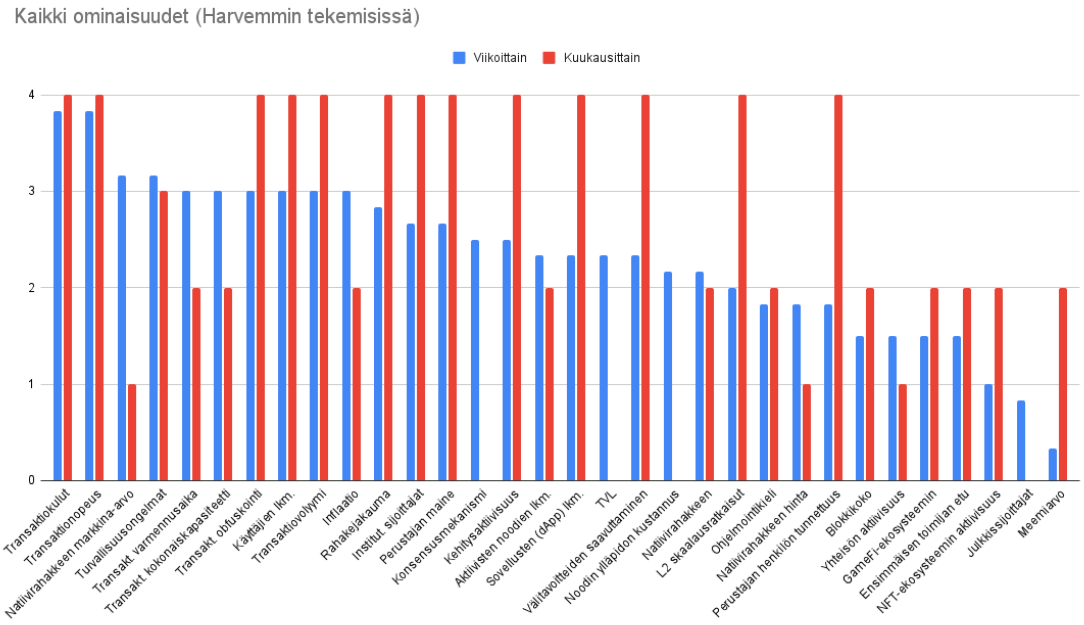
Kyselyyn vastanneista 78,8% kertoi olevansa päivittäin tekeimissä lohkoketjuteknologioiden ja kryptovaluuttojen parissa. Kyseisen vastaajajoukon tärkeimmässä pisteneljänneksessä olivat turvallisuusongelmat (3,15), transaktiokulut (3,08), perustajan maine (3,04), transaktionopeus (3,04) sekä kehitysaktiivisuus (3,00). Neljän kärki on sama listaus, kuin sijoittajat-vertailuryhmällä, jonka edustajat muodostivatkin 69,2% päivittäisistä käyttäjistä. 15,4% olivat kehittäjiä ja 15,4% kehittäjäsijoittajia.



Kuva 4.11: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso niiden kanssa päivittäin tekemisissä olevien keskuudessa

Viikoittain kryptojen parissa toimivia oli 18,2% vastaajista, joista 100% kuului myös sijoittajat-vertailuryhmään. Tärkeimpään pisteneljännekseen olivat valikoitu-

neet transaktiokulut (3,83) ja transaktionopeus (3,83) hyvin alhaisella keskihajonnalla (0,41). Muita tärkeitä ominaisuuksia olivat natiivirahakkeen markkina-arvo (3,17), turvallisuusongelmat (3,00), transaktioiden varmennusaika (3,00), transaktioiden kokonaiskapasiteetti (3,00), transaktioiden obfuskointi (3,00), käyttäjien lukumäärä (3,00), transaktiovolyymi (3,00) ja inflaatio (3,00). Listattuna oli useampikin tekijä, jotka eivät saaneet merkittävää suosiota esimerkiksi päivittäin kryptojen parissa toimivilta, kuten natiivirahakkeen markkina-arvo (vrt. 1,77) ja transaktioiden obfuskointi (vrt. 1,88).



Kuva 4.12: L1-lohkoketjujen ominaisuuksien keskimääräinen arvostustaso niiden kanssa viikoittain tai kuukausittain tekemisissä olevien keskuudessa

Kuukausittain tekemisissä olevien vastaukset erosivat merkittävästi muusta joukosta, sillä tärkeimpään kategoriaan olivat nousseet mm. L2 skaalausratkaisut (4,00) ja institutionaaliset sijoittajat (4,00) monen muun ominaisuuden muassa. Kyselyyn oli kuitenkin vastannut vain yksi kuukausittaisella frekvenssillä toimiva henki-

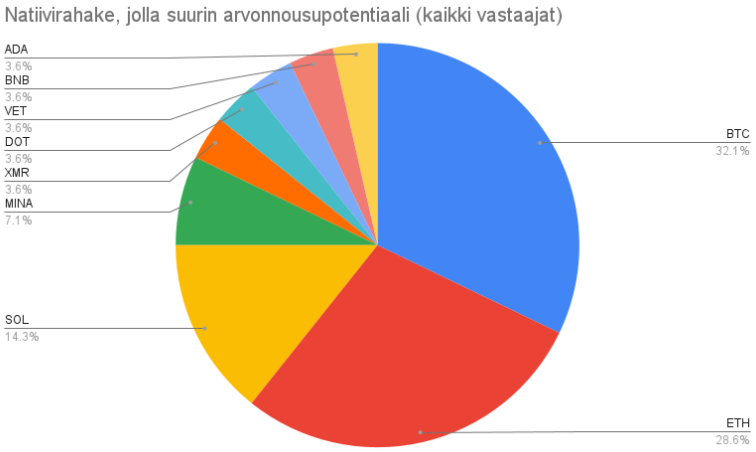
lö (3,3% vastaajista), joten tuloksia ei voida pitää kovin merkittävinä. Tarkempaa analyysiä ei kuukausittaisen aktiivisuuden osalta tehty.

4.3.3 Tulevaisuuden arviointi

Kyselyssä tiedusteltiin vastaajien näkemyksiä nykyisistä L1-ekosysteemeistä ja niiden tulevaisuuden kehityksestä kahdella kysymyksellä. Ensimmäiseksi kyselyyn osallistuneita pyydettin valitsemaan 1—4 L1-lohkoketjuprotokollaa, joiden ekosysteemeillä he näkivät parhaat menestymisen edellytykset. Kysymyksen tarkoituksena oli korostaa lohkoketjun asemaa kehitysalustana ja infrastruktuurina erilaisille hajautetuille sovelluksille. Toisessa kysymyksessä vastaajia pyydettiin valitsemaan yksi L1-lohkoketjun natiivirahake, jolla he arvioivat olevan parhaat edellytykset arvonnousuun kuluvan 5 vuoden aikana. Kysymyksen tarkoituksena oli korostaa erityisesti L1-lohkoketjujen ja niille ominaisten kryptovaluuttojen sovellusta sijoitusinstrumenttina. Vastauksia analysoitiin nominaaliasteikolla.

Tarkastellessa molempien kysymyksien vastatauksia koko vastausjoukon osalta, voidaan havaita näkemysten L1-protokollan kehityspotentiaalista korreloivan näkemyksestä kyseisten lohkoketjun natiivirahakkeiden arvonnousun kanssa, vaikka merkitseviä erojakin oli. Koko vastaajajoukon osalta eniten ekosysteemikasvua nähtiin olevan Ethereumilla (25,0% vastauksista), toiseksi eniten Bitcoinilla (19,6% vastauksista) ja kolmanneksi eniten Solanalla (14,3% vastauksista). Natiivirahakkeidenn arvonnousun osalta kärkikolmikossa olivat ediustettuna samat lohkoketjut, joskin arvokkaimpana rahakkeena nähtiin BTC (32,1%), toisena ETH (28,6%) ja kolmantena SOL (14,3%). Kysymykset eivät ole täysin verrannolisia keskenään, sillä vastaajia pyydettiin antamaan eri määrä vastauksia. Tästä voidaan kuitenkin päätellä TK2:n hengessä, että yleisesti tietyn lohkoketjun potentiaali kehityksen ja sijoittamisen osalta nähdään hyvin samankaltaisena.

Kuva 4.13: Arvio L1-lohkoketjuista, joiden ekosysteemeillä suurin kasvupotentiaali (kaikki vastaajat)

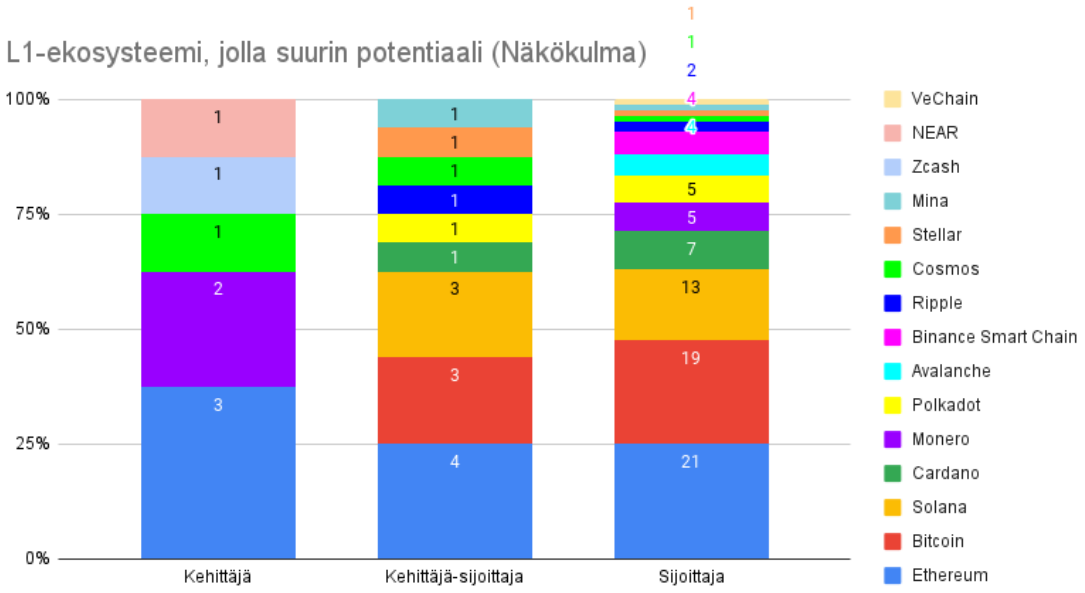


Kuva 4.14: Arvio natiivirahakkeiden suurimmista arvonousijoista 5v aikajänteellä (kaikki vastaajat)

L1-protokollat ja ekosysteemikehitys

Tarkastellessa eri vertailuryhmiä kaikkien näkökulmaryhmien vastauksissa Ethereum oli vahviten edustettuna L1-protokollien tulevaisuutta arvioitaessa. Sijoittajat ja kehittäjä-sijoittajat pitivät Bitcoinia toisiksi potentiaalisimpana ja Solanaa kol-

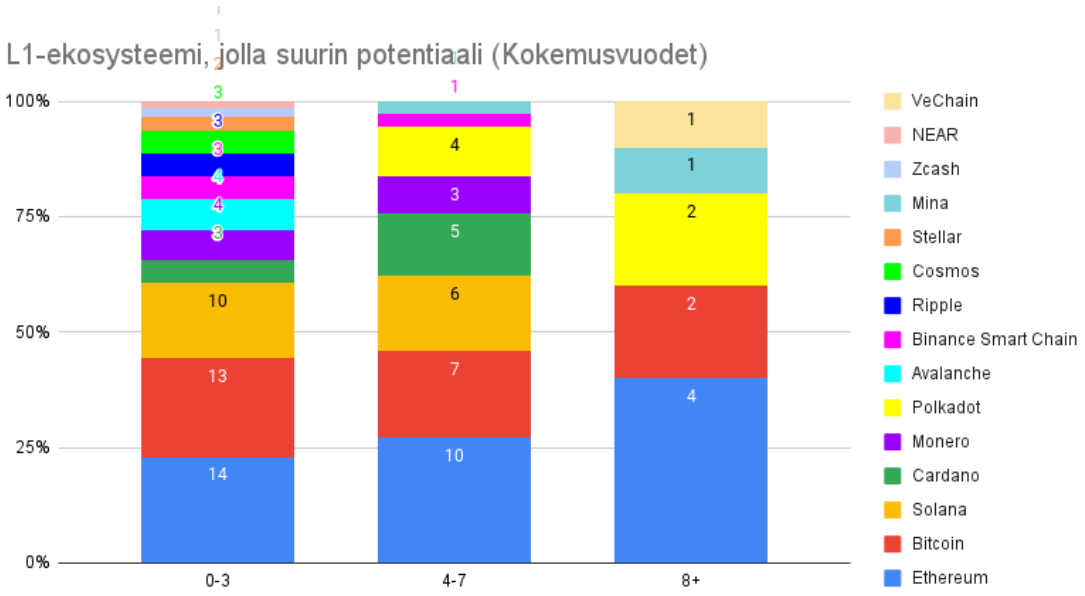
mantena. On huomioinarvoista, että yksikään kehittäjä ei uskonut Bitcoin-ekosysteemillä olevan parasta potentiaalia, kuten ei myöskään Solanalla. Kehittäjien toisella sijalla oli turvallisuuteen ja anonyymeihin transaktioihin erikoistunut Monero. Tulos osaltaan vastaa TK2:een korostaen kehittäjien ja sijoittajien eroavaisuuksia.



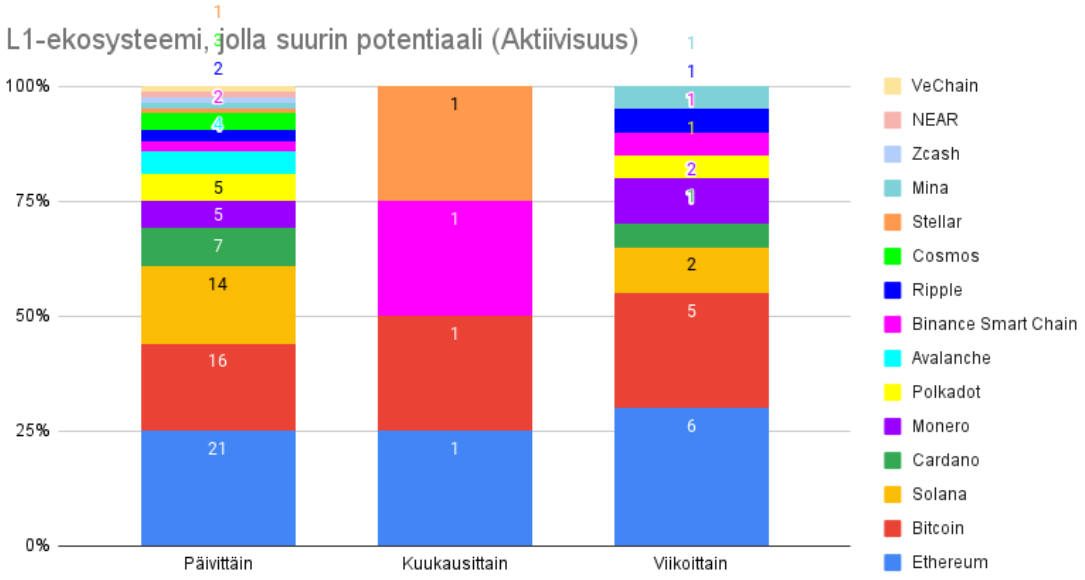
Kuva 4.15: L1-lohkoketjuekosysteemi, jolla vastaajat näkivät suurimman kasvupotentiaalin jaoteltu näkökulman mukaan

Tarkastellessa vastauksia kokemusvuosien tai aktiivisuuden mukaan, olivat erot vähäisempiä. Kaikkien ryhmien vastauksissa Ethereum oli vahviten edustettuna ja Bitcoin toiseksi eniten. Aktiivisuusryhmien osalta Solana oli saanut kolmennen sijan verran kannatusta päivittäin (15,9 %) ja viikoittain (10%) kryptojen kanssa tekemisissä olevien keskuudessa. Samaten kokemusvuosiryhmistä Solana oli kolmannella sijalla 0—3 kokemusvuotta (16,4%) sekä 4—7 kokemusvuotta omaavilla (16,2%). Yli kahdeksan kokemusvuotta omaavilla Polkadot oli kolmanneksi suosituin (22,2% vastauksista). Kysymyksen tulokset eivät osaltaan vahvistaneet TK3 tai TK4 käsitystä, että aktiivisuus tai kokemusvuodet merkittävästi vaikuttaisivat näkemyksiin

itse lohkoketjuprotokollien potentiaalia kohtaan.



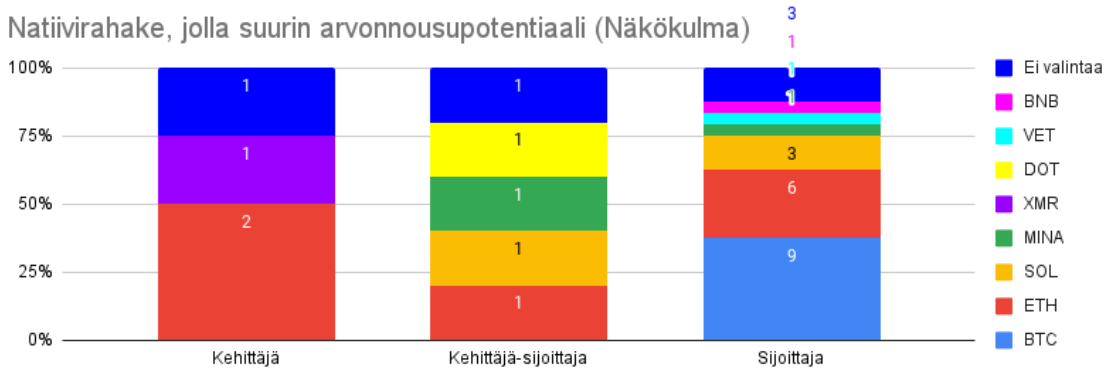
Kuva 4.16: L1-lohkoketjuekosysteemi, jolla vastaajat näkivät suurimman kasvupotentiaalin jaoteltu kokemusvuosien mukaan



Kuva 4.17: L1-lohkoketjuekosysteemi, jolla vastaajat näkivät suurimman kasvupotentiaalin jaoteltu aktiivisuuden mukaan

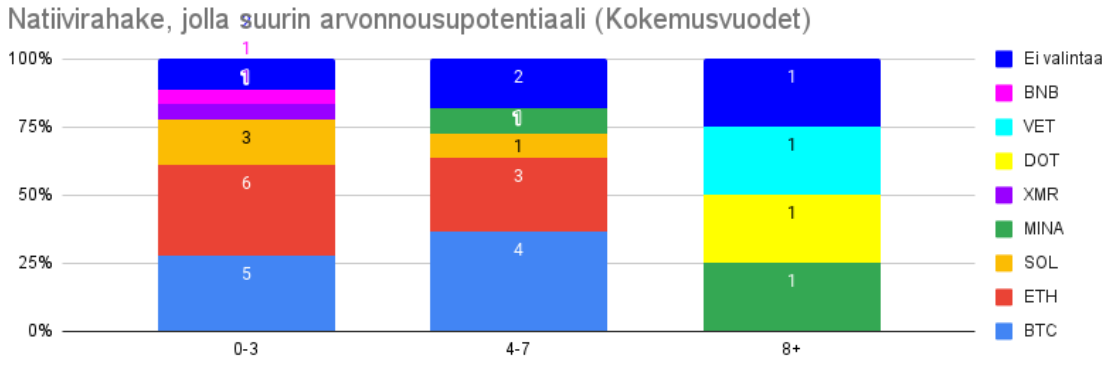
Natiivirahakkeet ja arvonnousu

Natiivirahakkeiden arvonnousupotentiaalia vertaillessa vertailuryhmien välillä syntyi myös eroja. Sijoittaja-ryhmässä suurin osa näki arvonnousupotentiaalia eniten bitcoinilla (40,9% vastaajista), ethereumilla (27,3% vastaajista) ja solanalla (13,7% vastaajista). Kehittäjät tai kehittäjä-sijoittajat eivät nähneet bitcoinilla samaa arvoa, vaan arvostivat eniten ethereumia (66,7% ja 25%). Tämän lisäksi kehittäjät arvostivat moneron arvonnousupotentiaalia (33,3%) ja kehittäjä-sijoittajat solanaa, minaa ja DOT:ia (kukin 25%).



Kuva 4.18: L1-lohkoketjun natiivirahake, jolla vastaajat näkivät suurimman arvonnousupotentiaalin jaoteltuna vastaajien näkökulmien mukaan

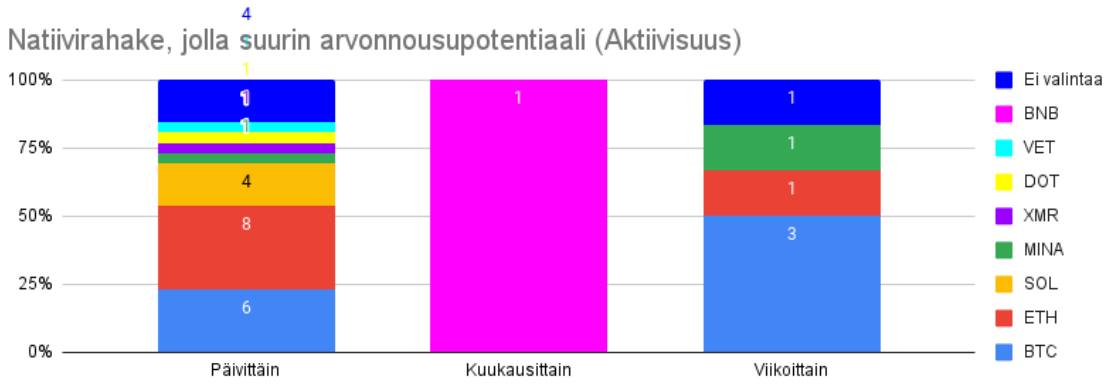
Kokemusvuosia arvioitaessa eniten kokemusvuosia (8+) omaavien ryhmällä oli suurempia näkemyseroja, sillä ETH ja BTC puuttuivat kokonaan. Suurin potentiaali nähtiin MINA, DOT ja VET -rahakkeilla. Vähemmän kokemusvuosia omaavien ryhmät arvioivat suurimmiksi nousijoiksi BTC:n, ETH:n ja SOL:n.



Kuva 4.19: L1-lohkoketjun natiivirahake, jolla vastaajat näkivät suurimman arvonnousupotentiaalin jaoteltuna vastaajien kokemusvuosien mukaan

Aktiivisuusryhmien suhteen ETH ja BTC olivat vahvasti edustettuina lukuun ottamatta kuukausittaisen aktiivisuuden ryhmää, jossa ainoa vastaus oli kohdistettu

BNB-rahakkeelle.



Kuva 4.20: L1-lohkoketjun natiivirahake, jolla vastaajat näkivät suurimman arvonnousu potentiaalinjaoteltuna vastaajien aktiivisuuden mukaan

Vertailuryhmät ovat sen verran pieniä, että tilastollista merkittävyyttä ei saavutettu. Tulokset antavat kuitenkin viitteitä TK2:n suhteen ja korostavat eroja kehittäjien ja sijoittajien välillä. Tulokset olisivat todennäköisesti olleet parempia, mikäli kysymyksenasettelu olisi vastannut edellistä L1-protokollien potentiaalia arvioinutta kysymystä.

5 Tutkimuksen tulokset ja johtopäätökset

Tutkimuksen selvitettiin, miten lohkoketjuteknologian ja kryptovaluuttojen parissa toimivat ihmiset antavat painoarvoa eri L1-lohkoketjujen ominaisuuksille. Tuloksia tarkasteltiin vastaajien motiivien ja lohkoketjuteknologioiden parissa vietettyjen kokemusvuosien sekä aktiivisuuden mukaan. Tutkimuksen avulla määriteltiin kullekin ominaisuudelle painoarvo, joita voi tarkastella kuvassa 4.4. Kyselyn tuloksien keskiarvoja voidaan suoraan käyttää kertoimina, mikäli eri ominaisuuksia verrataan samalla skaalalla ja niiden välistä suhdetta normalisoidaan ominaisuudelle keskimäärin annetun painoarvon suhteen.

Tutkimuksessa havaittiin myös selkeitä eroja eri vastausryhmien kesken. Esimerkiksi kehittäjät antoivat merkittävästi muita ryhmiä enemmän arvoa L1-lohkoketjujen teknisille ominaisuuksille, kuten lohkoketjun toimintalogiikan määrittelevälle konsensusmekanismille ja toteutuksen ohjelmointikielelle. Viiteryhmäkohtaisia painotuskertoimia voidaan helposti käyttää tutkimuksessa käsitellyille eri viiteryhmille.

Tutkimus oli rajattu L1-lohkoketjujen analysointiin, mikä rajasi pois merkittävän määrän kryptovaluuttoja, sovelluksia ja lohkoketjuja tutkimuksen piiristä. On todennäköistä, että samat vastaajat antaisivat L1- ja L2-protokollien samalle ominaisuudelle erilaisen painoarvon, mikäli sama kysely toistettaisiin keskittymällä L2-lohkoketjujen ominaisuuksiin.

Tutkimuksessa tutkittiin painoarvoa, jota vastaajat antavat eri L1-lohkoketjujen ominaisuuksille. Tutkimuksessa ei kuitenkaan selvitetty, millä tavalla ominaisuus vaikuttaa päätöksentekoon. Pääosasta käsiteltyjä ominaisuuksia suhtautuminen voidaan päätellä, sillä esimerkiksi korkeaa transaktiokapasiteettia sekä alhaisia transaktiokustannuksia voidaan pitää positiivisina elementteinä. Vastaavasti esimerkiksi konsensusmekanismin osalta, mille kehittäjät antoivat merkittävää painoarvoa, on monimutkaisempaa arvioida, milloin se tulkittaisiin päätöksenteon kannalta positiivisesti tai negatiivisesti. Kyselyä suunniteltaessa päätös oli tietoinen, sillä se haluttiin pitää mahdollisimman yksinkertaisena.

Tutkimuksessa kyselyyn vastanneilta ei tiedusteltu, mikäli he toimivat lohkoketjuteknologioiden parissa ammattimaisesti vai harrastuksenomaisesti. Kysymys olisi tuonut syvyyttä kyselyyn ja antanut merkittävää tietoa vastanneiden sitoutumisen asteesta lohkoketjuteknologioita ja kryptovaluuttoja kohtaan. Sama tavoite oli kyselyssä olleella aktiivisuuskysymyksellä, joskin jälkikäteen arvioiden kysymys ei ollut tarkoituksenmukainen. Jonkin teeman kanssa voi olla päivittäin tekemisissä, vaikka siihen syventymiseen ei merkittävästi käyttäisikään resurssejaan.

Tutkimuksen tuloksena saatiin muodostettua eri ominaisuuksille painotuskertoimet, joiden avulla voidaan helpommin määrittää miten paljon ihmiset antavat L1-lohkoketjujen eri ominaisuuksille painoarvoa. Kyseisiä painokertoimia voidaan hyödyntää jatkokehitettäessä mittaristoa, jolla vertaillaan L1-lohkoketjuja eri tarkoituksiin. Samoja painotuskertoimia voidaan hyödyntää myös esimerkiksi lohkoketjukehittäjien toimesta, kun he tekevät päätöksiä erilaisten teknisten komporomissien suhteen. Tutkimusta olisikin suoraviivaista jatkaa tekemällä kattava vertailu L1-protokollista yhtenäistetyllä mittaristolla ja tämän tutkimuksen tuloksena saaduilla painotuskertoimilla. Toinen suoraviivainen jatkotutkimuksen aihe, olisi tarkempi syventyminen L2-protokollien ominaisuuksiin.

Lähdeluettelo

[1] R. Merton ja Z. Bodie, "A CONCEPTUAL FRAMEWORK FOR ANALYZING THE FINANCIAL SYSTEM", *The Global Financial System: A Functional Perspective*, 1995.

[2] G. J. Benston ja C. W. Smith, "A transactions cost approach to the theory of financial intermediation", *The Journal of finance*, vol. 31, nro 2, s. 215–231, 1976.

[3] K.-C. Chen, "Implications of Fintech developments for traditional banks", *International journal of economics and financial issues*, vol. 10, nro 5, s. 227, 2020.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[5] V. Buterin et al., "A next-generation smart contract and decentralized application platform", *white paper*, vol. 3, nro 37, s. 2–1, 2014.

[6] M. Xu, X. Chen ja G. Kou, "A systematic review of blockchain", *Financial Innovation*, vol. 5, nro 1, s. 1–14, 2019.

[7] S. Nakamoto, *Bitcoin P2P e-cash paper*, (accessed: 02.07.2021). url: `https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html`.

[8] L. Lamport, R. Shostak ja M. Pease, "The Byzantine generals problem", teoksessa *Concurrency: the works of leslie lamport*, 2019, s. 203–226.

[9] W. Dai, *B-Money*, (accessed: 24.08.2021). url: http://www.weidai.com/bmoney.txt.

[10] H. Gilbert ja H. Handschuh, "Security analysis of SHA-256 and sisters", teoksessa *International workshop on selected areas in cryptography*, Springer, 2003, s. 175–193.

[11] S. Sayeed ja H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack", *Applied sciences*, vol. 9, nro 9, s. 1788, 2019.

[12] *THE HISTORY OF BITCOIN CASH*, (accessed: 22.07.2022). url: https://bitcoincash.org/.

[13] N. Szabo, "Smart contracts: building blocks for digital markets", *EXTROPY: The Journal of Transhumanist Thought,(16)*, vol. 18, nro 2, s. 28, 1996.

[14] K. Wu, "An empirical study of blockchain-based decentralized applications", *arXiv preprint arXiv:1902.04969*, 2019.

[15] *UNISWAP PROTOCOL*, (accessed: 20.09.2022). url: https://uniswap.org/.

[16] *AAVE LIQUIDITY PROTOCOL*, (accessed: 20.09.2022). url: https://www.aave.com/.

[17] *DECENTRALIZED ASSET MANAGER FOR WEB3*, (accessed: 20.09.2022). url: https://www.vanilladefi.com/.

[18] B. Raiter, *Turing Complete*, (accessed: 24.07.2022). url: https://wiki.c2.com/?TuringComplete.

[19] *ETHEREUM VIRTUAL MACHINE (EVM)*, (accessed: 12.09.2022). url: https://ethereum.org/en/developers/docs/evm/.

[20] S. Tikhomirov, "Ethereum: state of knowledge and research perspectives", teoksessa *International Symposium on Foundations and Practice of Security*, Springer, 2017, s. 206–221.

[21] *DApp Statistics*, (accessed: 20.09.2022). url: `https://www.stateofthedapps.com/stats/platform/ethereum#new`.

[22] F. Suarez ja G. Lanzolla, "The half-truth of first-mover advantage", *Harvard business review*, 2005.

[23] J. Abadi ja M. Brunnermeier, "Blockchain economics", National Bureau of Economic Research, tekninen raportti, 2018.

[24] K. Azbeg, O. Ouchetto, S. Jai Andaloussi ja L. Fetjah, "An overview of blockchain consensus algorithms: comparison, challenges and future directions", *Advances on smart and soft computing*, s. 357–369, 2021.

[25] C. Lee, *Litecoin (2011)*, (accessed: 28.11.2022), 2011. url: `https://ataix.com/assets/currencies/Lite-Coin-Whitepaper.pdf`.

[26] M. J. Krause ja T. Tolaymat, "Quantification of energy and carbon costs for mining cryptocurrencies", *Nature Sustainability*, vol. 1, nro 11, s. 711–718, 2018.

[27] *Bitcoin Total Hash Rate (TH/s)*, (accessed: 16.10.2022). url: `https://www.blockchain.com/explorer/charts/hash-rate`.

[28] QuantumMechanic, *Proof of stake instead of proof of work*, (accessed: 16.10.2022). url: `https://bitcointalk.org/index.php?topic=27787.0`.

[29] S. King ja S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake", *self-published paper, August*, vol. 19, nro 1, 2012.

[30] N. Community, "Nxt Whitepaper", 2014.

[31] P. Vasin, "Blackcoin's proof-of-stake protocol v2", *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.

[32] CLains, *Delegated Proof of Stake (DPOS) White Paper by Daniel Larimer*, (accessed: 28.11.2022). url: `https://bitcointalk.org/index.php?topic=558316.0`.

[33] I. Grigg, "EOS-An Introduction", 2017.

[34] T. DAO, "Tron - Advanced Decentralized Blockchain Platform", 2018.

[35] V. Zamfir, *Introducing Casper "the Friendly Ghost"*, (accessed: 28.11.2022). url: `https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost`.

[36] A. Kiayias ja A. Russell, "Ouroboros-bft: A simple byzantine fault tolerant consensus protocol", *Cryptology ePrint Archive*, 2018.

[37] J. Kwon ja E. Buchman, "Cosmos whitepaper", *A Netw. Distrib. Ledgers*, 2019.

[38] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework", *White Paper*, vol. 21, s. 2327–4662, 2016.

[39] S. Kim, Y. Kwon ja S. Cho, "A survey of scalability solutions on blockchain", teoksessa *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, 2018, s. 1204–1207.

[40] D. Mechkaroska, V. Dimitrova ja A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of blockchain technology", teoksessa *2018 26th Telecommunications Forum (TELFOR)*, IEEE, 2018, s. 1–4.

[41] *SolanaFM - A friendly Solana explorer.* (accessed: 09.12.2022). url: `https://solana.fm/?cluster=mainnet-qn1`.

[42] J. Göbel ja A. E. Krzesinski, "Increased block size and Bitcoin blockchain dynamics", teoksessa *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, IEEE, 2017, s. 1–6.

[43] P. Wackerow et al., *BLOCKS*, (accessed: 10.12.2022). url: `https://ethereum.org/en/developers/docs/blocks/#block-size`.

[44] *Ethereum Average Block Time Chart*, (accessed: 11.11.2022). url: `https://etherscan.io/chart/blocktime`.

[45] D. C. North ja D. C. North, *Transaction costs, institutions, and economic performance*. ICS Press San Francisco, CA, 1992.

[46] E. Lombrozo, J. Lau ja P. Wuille, *Segregated Witness (Consensus layer)*, (accessed: 30.11.2022), 2015. url: `https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki`.

[47] *Sharding*, (accessed: 30.11.2022). url: `https://ethereum.org/en/upgrades/sharding/`.

[48] *What is layer 2?*, (accessed: 30.11.2022). url: `https://ethereum.org/en/layer-2/`.

[49] X. Li, P. Jiang, T. Chen, X. Luo ja Q. Wen, "A survey on the security of blockchain systems", *Future Generation Computer Systems*, vol. 107, s. 841–853, 2020.

[50] M. Raikwar, D. Gligoroski ja K. Kralevska, "SoK of used cryptography in blockchain", *IEEE Access*, vol. 7, s. 148 550–148 575, 2019.

[51] Q. Lin, C. Li, X. Zhao ja X. Chen, "Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities", teoksessa *2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW)*, IEEE, 2021, s. 80–87.

[52] Y. Jia, C. Xu, Z. Wu, Z. Feng, Y. Chen ja S. Yang, ”Measuring Decentralization in Emerging Public Blockchains”, teoksessa *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 2022, s. 137–141. DOI: 10.1109/IWCMC55113.2022.9825341.

[53] F. A. Farris, ”The Gini index and measures of inequality”, *The American Mathematical Monthly*, vol. 117, nro 10, s. 851–864, 2010.

[54] *Run an Avalanche Node with Microsoft Azure*, (accessed: 18.11.2022). url: https://docs.avax.network/nodes/build/set-up-an-avalanche-node-with-microsoft-azure.

[55] *Validator Requirements*, (accessed: 18.11.2022). url: https://docs.solana.com/running-validator/validator-reqs.

[56] H. Yousaf, G. Kappos ja S. Meiklejohn, ”Tracing transactions across cryptocurrency ledgers”, teoksessa *28th USENIX Security Symposium (USENIX Security 19)*, 2019, s. 837–850.

[57] *Tornado Cash Github Repository*, (accessed: 14.11.2022). url: https://github.com/tornadocash.

[58] D. Yaffe-Bellany, ”Treasury Dept. blacklists crypto platform used in money laundering.”, *The New York Times*, 8. elokuuta 2022. url: https://www.nytimes.com/2022/08/08/technology/treasury-blacklist-crypto-tornado-cash-laundering.html (viitattu 14. 11. 2022).

[59] J. Silberholz ja D. A. Wu, ”Measuring Utility and Speculation in Blockchain Tokens”, *Available at SSRN 3915269*, 2021.

[60] *Reliable Vote Transmission*, (accessed: 01.12.2022). url: https://docs.solana.com/implemented-proposals/reliable-vote-transmission#performance.

[61] M. Shen, A. Garg, C. Spencer, E. Herreros ja K. Deeter, ”Electric Capital Developer Report January - December 2021”, Electric Capital Ltd, tammikuu 2022.

[62] C. Britton, ”Choosing a programming language”, *Microsoft MSDN library, available via https://msdn. microsoft. com/enus/library/cc168615. aspx*, 2008.

[63] *Contributions to develop, excluding merge commits and bot accounts*, (accessed: 24.07.2022). url: `https://github.com/ethereum/solidity/graphs/contributors`.

[64] E. Yazdanparast, *List of programming languages and frameworks used in 41 crypto projects*, (accessed: 16.07.2022), tammikuu 2022. url: `https://medium.com/coinmonks/list-of-programming-languages-and-frameworks-used-in-41-crypto-projects-2b7223099c57#7fc4`.

[65] *Cryptocurrency prices, charts and market capitalizations*, (accessed: 16.07.2022). url: `https://coinmarketcap.com/`.

[66] K. Korakitis ja R. Muir, ”Slashdata State of the Developer Nation 22nd Edition”, Slashdata Ltd, huhtikuu 2022.

[67] *Remote Solidity developer jobs with U.S. companies*, (accessed: 16.07.2022). url: `https://www.turing.com/jobs/remote-solidity-developer`.

[68] R. Watson, ”Quantitative research”, *Nursing Standard (2014+)*, vol. 29, nro 31, s. 44, 2015.

[69] I. R. Hallberg, ”Surveys”, *Nursing research: Designs and methods*, s. 179–189, 2008.

[70] A. O. Sykes, ”An introduction to regression analysis”, 1993.

[71] W. G. Cochran, ”Analysis of covariance: its nature and uses”, *Biometrics*, vol. 13, nro 3, s. 261–281, 1957.

[72] R. FISHEE, ”Statistical Methods for Research Workers, (1932)”, *Edinburgh and London: Oliver and Boyd*,

[73] S. Peters, *Do you know who your stakeholders are?*, (accessed: 28.06.2022). url: `https://conferences.oreilly.com/oscon/oscon-or-2018/public/schedule/detail/66945.html`.