TURUN YLIOPISTO

Ethereumin skaalaaminen

LuK-tutkielma
Turun yliopisto
Tietotekniikan laitos
Tietojenkäsittelytieteet
Tammikuu 2022
Aleksi Runola

Turun yliopisto
Tietotekniikan laitos / Teknillinen tiedekunta

ALEKSI RUNOLA: Ethereumin skaalaaminen

LuK-tutkielma
Tietojenkäsittelytieteet
Tammikuu 2022

Tämä tutkielma käsittelee Ethereumia, lohkoketjuja eli teknologiaa, jonka päällä se toimii sekä Ethereumin skaalaamiseen käytettyjä ja tulevaisuudessa käytettäviä tekniikoita. Ethereum on alusta hajautetuille sovelluksille ja sen skaalaaminen on tarpeellista verkon suosion ja tätä kautta myös kustannusten kasvaessa.

Tällä hetkellä suosituimpiin ja potentiaalisimpiin skaalaustekniikoihin kuuluvat sivu- ja Plasma-ketjut, sirpalointi, optimistiset ja ZK-rollupit sekä Proof-of-Stake-konsensusmekanismiin siirtyminen. Tässä tutkimuksessa tarkastellaan näitä tekniikoita pääasiallisesti skaalaustrilemman kolmesta eri näkökulmasta: turvallisuus, hajautettuneisuus ja skaalautuvuus.

Eri tekniikoista sirpalointi on ainoa tapa, joka skaalaa itse lohkoketjua todellisesti säilyttäen skaalaustrilemman eri osa-alueet eheänä. Myös rollupit ovat tarjoavat skaalautuvuutta ja turvallisuutta, mutta vaikka sen pohjana käytetty Ethereumin lohkoketju on hajautettu, itse skaalaus tapahtuu ainakin toistaiseksi keskitettyjen tahojen toimesta. Tutkimuksessa kuitenkin todetaan, että kaikille skaalausratkaisulle löytyy Ethereumin ekosysteemistä oma paikkansa eri tarkoituksiin.

Asiasanat: Ethereum, skaalaaminen, sivuketjut, rollupit, sirpalointi

Sisällysluettelo

Kuvaluettelo

1 Johdanto

Ethereum on lohkoketjuteknologiaan perustuva alusta, jonka päälle voi rakentaa hajautettuja sovelluksia. Nämä sovellukset ovat erityisen hyödyllisiä tarkoituksiin, joissa vaaditaan turvallisuutta ja luotettavuutta, kuten varojen siirtoa tokenien avulla tai hajautettujen autonomisten organisaatioiden hallintaa. Tämä on mahdollista Ethereumin päällä sen sisäänrakennetun Turing-täydellisen ohjelmointikielen ansiosta. Lohkoketjuteknologiaa ja Ethereumia esitellään syvemmin luvussa 2. [1]

Ethereumin transaktioihin ja sovellusten luomiseen tai käyttämiseen käytettävän polttoaineen, etherin hinta on kasvanut pelkästään viimeisimmän vuoden aikana yli kuusinkertaiseksi. Lisäksi polttoainetta vaadittava määrä kasvaa verkon suosion kasvaessa, mistä johtuen Ethereumin kuluttajaystävällisyyttä on kritisoitu. [2] Tätä ongelmaa sekä verkon yleisen käytön kasvua varten on kehitetty ja kehitetään erilaisia skaalausratkaisuja.

Skaalausratkaisuja voidaan käydä läpi kolmelta eri kannalta:

1. Turvallisuus
2. Hajautettuneisuus
3. Skaalautuvuus

Näiden kolmen sanotaan muodostavan skaalaustrilemman eli ongelman, jossa näitä kaikkia ei olla vielä pystytty ratkaisemaan. Tässä tutkielmassa tutkitaan tämänhetkisiä ja tulevaisuuden skaalausratkaisuja trilemman kaikista näkökulmista. Tämä mahdollistaa päätelmien tekemisen skaalausratkaisujen sopivuudesta eri tarkoituksiin, sekä asettaa skaalausratkaisuja tietyllä tapaa paremmuusjärjestykseen. Ihannetilanteessa skaalausratkaisu pystyisi ratkomaan kaikki trilemman kolme näkökulmaa.

Tutkielman luvussa 2 perehdytään lohkoketjuihin ja niiden tärkeimpiin elementteihin. Lohkoketjuihin perehtyminen tapahtuu pääasiassa Ethereumin ja sen ekosysteemin perspektiivistä. Luvussa 3 käsitellään Ethereumin eri skaalautuvuusratkaisuja ja niiden hyviä sekä huonoja puolia. Lopuksi luvussa 4 esitetään tutkielman yhteenveto ja johtopäätökset.

2 Ethereum

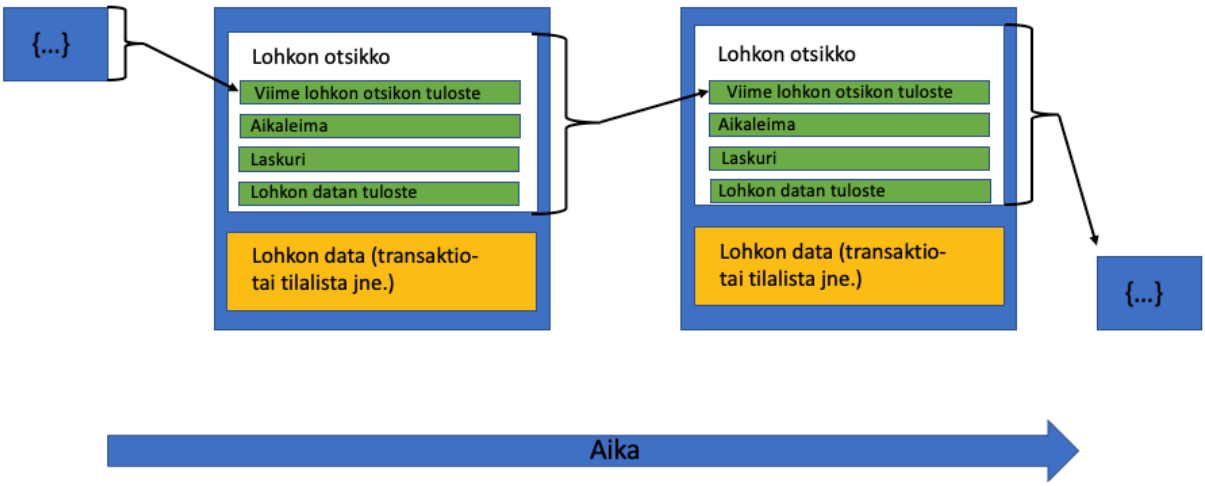
Tässä luvussa esitellään lohkoketjuja, Ethereumia ja sen päälle rakentunutta ekosysteemiä. Luku kertoo tarpeellisia perustietoja sekä -käsitteitä Ethereumin skaalaamisen käsittelyä varten luvussa 3.

2.1 Lohkoketjuista yleisesti

Lohkoketjut (blockchain) ovat hajautettuja digitaalisia tilikirjoja (ledger), jotka mahdollistavat tapahtumien tallentamisen ilman pankkia, valtiota tai muuta keskitettyä viranomaista. Tilikirja toimii siis tietokantojen tilalla ja sinne voidaan tallentaa dataa luottamatta välikäsiin tai kolmansiin osapuoliin. Vanhan datan paikkansapitävyyden voi tarkistaa uniikista tulosteesta, joka tuotetaan hajautusalgoritmin (hashing algorithm) avulla. Tulostetta voidaan kutsua myös nimellä hajautusarvo (hash value). Pienikin, jopa yhden bitin muutos, aiheuttaa tulosteen täyden muodonmuutoksen. Tätä havainnollistetaan kuvissa 1 ja 2. Lukemattomat nodet eli eräänlaisina palvelimina toimivat solmupisteet ylläpitävät lohkoketjuverkkoa. Nodeja käsitellään tarkemmin luvussa 3. Tässä kappaleessa esitelty vertaisverkkomalli mahdollistaa verkon turvallisuuden poistamalla vaaran yksittäisiin palvelimiin kohdistetuista hyökkäyksistä. [3]

Syöte	Tuloste
Tämä on syöte.	be504306f22603f6337c108cb83ac07e2aa0d653a6b1bbaf66b6ebab12e3c1b7
Tämäkin on syöte.	c08e9045e4c347402f0e951de14f7bd2572bac19b0260380441fc00f97c870d0

Kuva 1: SHA-256-hajautusalgoritmin tuottamat täysin erilaiset tulosteet kahdelle samankaltaiselle syötteelle.



Kuva 2: Yleinen malli lohkoketjun rakenteelle.

Ensimmäinen lohkoketjuteknologiaa hyödyntävä sovellus, kryptovaluutta Bitcoin, esiteltiin vuonna 2008 ja sen ensimmäinen lohko louhittiin vuonna 2009. Se toimii puhtaasti digitaalisena valuuttana, jonka tilikirja kirjaa kaikkien jo louhittujen bitcoinien osoitteista kirjaa. Ethereum luotiin vaihtoehtoiseksi protokollaksi tuomaan lohkoketjuteknologian ympärille uusia ominaisuuksia, joita ei olisi voitu toteuttaa Bitcoinin lohkoketjuverkossa. Ethereumin perustaja Vitalik Buterin julkaisi Ethereum Whitepaperin eli ko. projektia kuvailevan dokumentin vuonna 2013. Itse projekti julkaistiin 2015, minkä jälkeen se on kehittynyt nykyiseen, hieman alkuperäisestä eroavaan muotoonsa useiden muiden yhteisövetoisten, avoimeen lähdekoodiin perustuvien projektien tavoin. [1]

2.2 Ethereumin toimintaperiaatteet

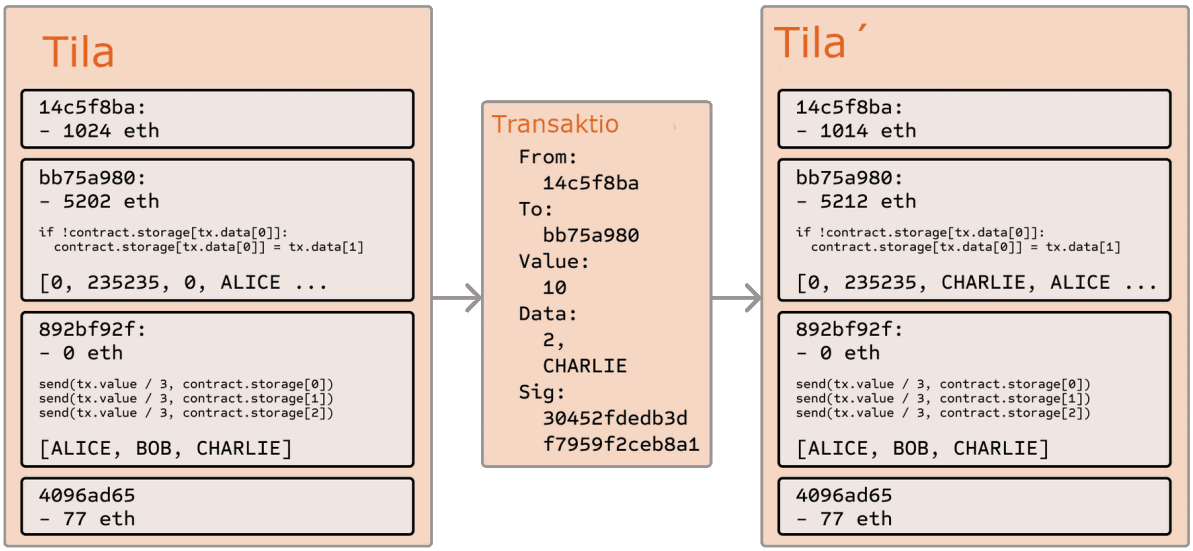
Ethereumin tarkoituksena on tarjota hajautettujen sovellusten rakentamiseen peruskerros, joka mahdollistaa nopean kehitystyön, tehokkaan tavan olla vuorovaikutuksessa muiden osoitteiden ja älysopimusten kanssa sekä kyseisten sovellusten turvallisuuden. Ethereum tekee tämän tarjoamalla lohkoketjun, jossa on sisäänrakennettu Turing-täydellinen ohjelmointikieli, jonka avulla voidaan luoda hajautettuja älysopimuksia eli Ethereumin päälle luotuja sovelluksia hyvinkin pienellä määrällä koodia. [1]

Älysopimuksilla pystytään luomaan tietokoneohjelmia tarkoituksiin, joilla on suurin tarve oikeellisuuden varmistukselle, kuten hajautettuja lainoja tai muita kahden osapuolen välisiä sopimuksia. Ethereumin älysopimukset ovat luonteeltaan julkisia ja muuttumattomia ja hallinnoivat usein arvokkaita omaisuuseriä. [4] Älysopimukset kirjoitetaan Javascriptin kaltaisella kielellä nimeltään Solidity, joka käännetään tavukoodiksi (bytecode). Tavukoodi

suoritetaan Ethereumin virtuaalikoneessa (Ethereum Virtual Machine, EVM), joka toimii Ethereumin lohkoketjun päällä. [5] Solidityn kääntämisestä tavukoodiksi huolimatta yksi EVM:n ongelmista on sen muistin käytön mukana aiheutuvat älysopimuksen suorituskustannukset, jotka maksetaan etherissä eli Ethereumin pääverkon (mainnet) polttoaineena (gas) toimivana valuuttana. [4]

EVM:n datan mallintaminen käsittää kaksi erilaista tallennustilaa: muistin (memory) sekä varastomuistin (storage). Muisti on välillinen ja se nollataan jokaisen transaktion alkaessa, kun taas varastomuisti on pysyvää tiedon tallentamista Ethereumin lohkoketjuun.[4] Jokaisella tilillä Ethereumin tilaperusteisessa (state) lohkoketjussa on oma varastomuistinsa, ja se on yksi Ethereum-tilin neljästä komponentista. Muut ovat uusintahyökkäyksiltä (replay attack) suojaava inkrementoiva laskuri (nonce)[6], tilin nykyinen saldo sekä tilin mahdollinen sopimuskoodi (contract code). Tilejä on kahdenlaisia: ulkoisesti omistettuja, yksityisillä avaimilla hallittavia tilejä sekä sopimustilejä (contract account), joita hallitaan niiden sopimuskoodin kautta. [1] Sopimustilien on mahdollista kutsua muiden älysopimusten funktioita, mutta kaikkien toimintojen aivan ensimmäisenä käynnistäjänä on toiminut ulkoisesti hallittava tili [7].

Tilien tekemät tapahtumat luokitellaan viesteihin ja transaktioihin. Ulkoisesti hallittavien tilien tapahtumat ovat transaktioita ja ne sisältävät vastaanottajan, yksityisavaimen kanssa suoritettavan allekirjoituksen, lähetettävän etherin määrän, vapaavalintaisen tietokentän, polttoaineen limiitin sekä polttoaineen hinnan. Sopimustilien tapahtumat ovat sen sijaan viestejä ja ne sisältävät transaktioiden kanssa samat komponentit pois lukien polttoaineen limiitin, koska älysopimuksen alkuperäisessä aktivoinnissa se on jo määritelty ja limiitin mukaisen polttoaineen määrän tulee riittää koko tapahtumaketjun suorittamiseen, jotta yksikään tapahtuma toteutuu. [1]



Kuva 3: Esimerkki Ethereumin tilan muutoksesta yksinkertaisen transaktion jälkeen. Jokaisella tilillä on oma saldonsa. [1]

2.3 Käyttötarkoitukset

Sopimustilejä hallitsee siis koodi, joita kutsutaan älysopimuksiksi (smart contract). Kryptografi Nick Szabo määritti termin älysopimus 1990-luvulla sanoen niiden olevan ”joukko digitaalisessa muodossa määriteltyjä lupauksia, mukaan lukien protokollat, joiden puitteissa osapuolet täyttävät muut lupaukset”.[8] Koska Ethereumin sisäänrakennettu kieli on Turing-täydellinen, on älysopimusten rajoitteena vain käyttäjän ohjelmointitaidot ja luovuus. [9]

Hajautetuksi sovellukseksi (decentralized app, dapp) kutsutaan sellaista sovellusta, jonka backend-koodi toimii hajautetun vertaisverkon (Ethereum) päällä. Tämä backend-koodi on siis älysopimus, joka tuo kaikki Ethereumin hyödyt mukanaan turvaamaan kyseistä hajautettua sovellusta. [10] Hajautettujen sovellusten potentiaalia hyödynnetään jo hyvin laajalla rintamalla eri alueille, kuten hajautettuun rahoitukseen (Decentralized Finance, DeFi), erinäisiin yritysratkaisuihin, pelialaan sekä digitaalisiin keräilyhyödykkeisiin. Hajautettujen sovellusten avuksi on kehitetty erinäisiä standardeja dokumentoimaan yhteentoimivuutta muiden sovellusten kanssa. [11], [12]

Seuraavaksi tutkielmassa esitellään pintapuoleisesti näitä käyttötarkoituksia hyödyntäen seuraavia käsitteitä [12]:

- Token edustaa lohkoketjun päällä olevaa asiaa. Asia voi olla mitä tahansa, kuten esimerkiksi rahaa, palveluita, osakkeita tai virtuaalinen lemmikki. Tokenien avulla pystymme tarjoamaan älysopimuksille mahdollisuuden olla vuorovaikutuksessa näiden hyödykkeiden kanssa. Tokeneilla on omat älysopimuksensa, joista selviää kunkin käyttäjän kyseisen tokenin saldo: tokenien lähettäminen tililtä toiseen on siis käytännössä vain saldojen päivittämistä tokenin omassa älysopimuksessa.
- ERC-standardit ovat Ethereum-yhteisön luomia standardeja tokenien sopimuksille, jotta ne voivat olla interaktiivisia muiden sopimusten kanssa.
    - ERC20 on yleisin, hyvin yksinkertainen standardi ei-uniikeille tokeneille. ERC20-standardin mukainen token on täysin samanvertainen muiden saman älysopimuksen tokenien kanssa, eikä sillä ole mitään erikoisoikeuksia tai -ominaisuuksia liitettynä.
    - ERC721 on standardi uniikeille tokeneille. Näistä lisää NFT:eiden yhteydessä.
    - ERC1155 on standardi, joka mahdollistaa yhdellä token-sopimuksella sekä uniikkien että ei-uniikkien tokenien edustamisen.

DeFi on yleinen termi talouteen liittyville tuotteille ja palveluille Ethereumin päällä. DeFin avulla loppukäyttäjät voivat muun muassa ottaa tai antaa lainaa, käydä kauppaa tokeneilla tai optioilla, ostaa vakuutuksia tai ansaita korkotuottoja erinäisissä muodoissa. Useimmin kaupankäyntivälineenä toimivat tokenit ovat ERC20-standardin mukaisia tokeneita. [13], [14]

Yleisimpänä yritysratkaisuna Ethereumin päällä toimii hajautettu autonominen organisaatio (Decentralized autonomous organization, DAO). DAO:t toimivat tietynlaisina internet-natiiveina yrityksinä, joita hallitsevat ja jotka omistavat niiden jäsenet. DAO:illa on usein oma rahastonsa (treasury), joihin kellään ei ole yksittäin pääsyä ilman ryhmän hyväksyntää. Päätökset DAO:issa tehdään äänestämällä käyttämällä äänivallan määrittäjänä jotain tokenia, joka on useimmiten ERC20-standardin mukainen.

NFT:t (non-fungible token) eli uniikkeja ominaisuuksia omaavat tokenit voivat edustaa useita eri kohteita niin virtuaalisessa kuin reaalimaailmassa. Näitä kohteita voivat olla esimerkiksi digitaalinen taide ja musiikki, liput konserttiin, tokenisoituja laskuja tai kiinteistöjä. NFT:n

ERC-standardi on ERC721, joka voi sisältää muun muassa metadataa tehden siitä monikäyttöisemmän standardin. ERC721:tä käytetään myös pelialalla, jolloin NFT:n kohteena voi olla esimerkiksi pelihahmo. Toinen pelialalla käytettävä standardi on ERC1155, joka mahdollistaa myös ei-uniikit tokenit, mikä luo säästöä Ethereumin polttoainekustannuksissa yhden älysopimuksen riittäessä useampaan eri kohteeseen.[15]–[17]

3 Skaalautuvuusratkaisut Ethereumissa

Yksi yleisistä Ethereumiin liittyvistä huolista on sen skaalautuvuus. Bitcoinin tapaan Ethereumin pääverkossa kaikki transaktiot tulee prosessoida jokaisen noden toimesta.[1] Ethereumilla on käytössä kolme erilaista nodea [18]:

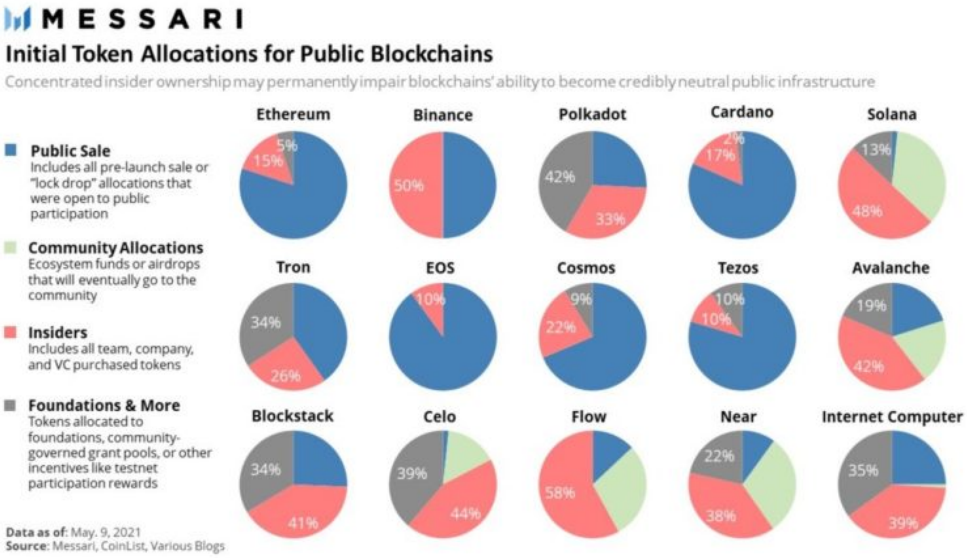
- Full nodet säilövät koko lohkoketjun datan. Full nodet ovat ainoita, jotka osallistuvat lohkojen validointiin sekä verifiointiin ja niiden tulee tallettaa koko lohkoketjun historian tilojen data itseensä. Jokainen tila ja tila' voidaan johtaa full nodesta (ks. Kuva 3). Full node pystyy myös tarjoamaan lohkoketjun dataa pyynnöstä.

- Light nodet säilövät pelkästään otsikot (ks. Kuva 1) ja noutavat muun datan pyyntöjen avulla. Light nodet pystyvät validoimaan datan lohkon otsikoiden perusteella, mutta ne eivät osallistu validointi- tai verifiointiprosesseihin. Light nodet ovat käytännöllisiä esimerkiksi laitteisiin, joihin ei mahdu useita gigatavuja lohkoketjun dataa.

- Archive nodet säilövät kaiken full noden sisällön ja luovat sen vanhoista tiloista arkiston. Näihin arkistoihin voidaan tehdä pyyntö historiallisista saldoista tai transaktioista vaikkapa lohkossa #4 000 000, ja saada nopea ja luotettava vastaus. Koko lohkoketjun arkistoiminen voi viedä useita teratavuja muistia, minkä takia keskivertokäyttäjien keskuudessa archive nodet eivät ole kovinkaan suosittuja. Niillä on kuitenkin käyttöä mm. lohkoketjun analytiikkatyökaluissa sekä lohkojen tutkintatyökaluissa (block explorer).

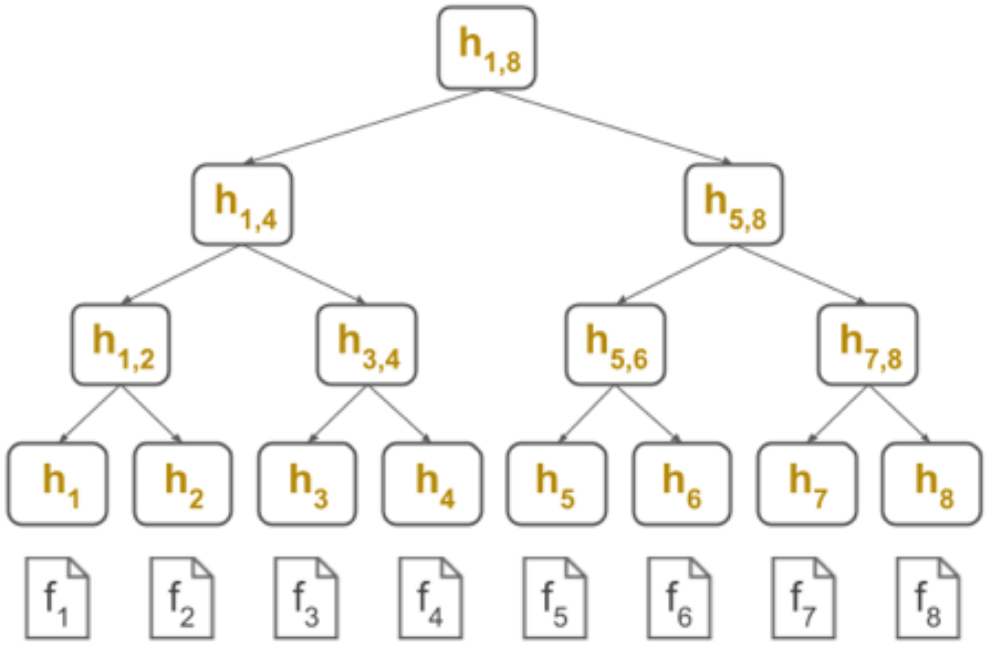
Full nodejen muistivaatimusten kasvaminen on yksi syy skaalautuvuuden tarpeelle, koska liian suuri lohkoketjun koko aiheuttaa keskitettyneisyyden (centralization) riskin. Tämä riski johtuisi siitä, että vain suurilla yrityksillä olisi mahdollista ylläpitää full nodeja, kun taas kaikkien normaalien käyttäjien tarvitsisi käyttää light nodeja. Toinen syy skaalautuvuuden tarpeelle on Ethereumin pääverkon kova kysyntä, joka johtaa hitaampiin transaktioihin ja käyttöä rajoittaviin polttoainekustannuksiin. Vaikka suoritustehon ja nopeuden lisääminen on tärkeää, tulee myös muistaa, että skaalausratkaisujen on tärkeää olla tinkimättä niiden hajautettuneisuudesta tai turvallisuudesta. Käsitteellisesti skaalaus voidaan luokitella lohkoketjussa tapahtuvaan skaalaamiseen (on-chain scaling) sekä lohkoketjun ulkopuolella tapahtuvaan skaalaamiseen (off-chain scaling). [1], [19]

Hajautettuneisuuden ja turvallisuuden mittaaminen lohkoketjuissa ei ole täysin yksiselitteistä. Niitä voidaan kuitenkin vertailla eri mittareilla, kuten validaattorien (validator) määrällä. Ethereumin pääverkossa on tarkasteluhetkellä (29.11.2021) 2984 full nodea [20], jotka siis toimivat validaattoreina. Toiseksi suurin Ethereumin kaltainen lohkoketju on siellä olevien varojen määrän perusteella Binance Smart Chain [21], jossa tarkasteluhetkellä toimii aktiivisena 21 validaattoria [22]. Tämä kertoo huomattavasta keskitettyneisyydestä, joka on aina riski lohkoketjun turvallisuudelle mm. virheellisten saldojen tai transaktioiden vahvistusten vuoksi. [23] Lohkoketjussa olevien varojen perusteella kolmanneksi suurin Ethereumin kaltainen lohkoketju, Solana [24] puolestaan omaa suuren määrän validaattoreita, tarkasteluhetkellä 1249 [25], mutta validointi ei ole mahdollista kenelle tahansa. Solanan validaattori kuluttaa 1,1 SOL:ia, Solanan natiivia valuuttaa vuorokaudessa, mikä kasvaa tarkasteluhetken kurssilla [26] yli 80 000 dollarin kustannukseksi vuodessa. Solanan tarkasteluhetken vuotuisella 7,53%:n [27] validaattoripalkkiolla tulisi validaattorin siis tässä PoS-konsensuksen (Proof-of-Stake) omaavassa lohkoketjussa steikata (stake) reilusti yli miljoonan dollarin edestä SOL:ia ollakseen kannattavaa. Solanalla on käytössään tukiohjelma, jonka avulla validaattori voi saada SOL:ia validoimisestaan, mutta tukiohjelmakin toimii keskitetysti Solanan taustalla olevan Solana Foundationin ohjaamana. Myös tokenien alkuperäinen allokaatio on Solanassa huomattavasti keskitetympää kuin Ethereumissa, Solana Labsin jäsenten sekä pääomasijoitusyritysten omistaen 48% kaikista tokeneista, kuten kuvasta 4 voidaan todeta. Tokenien keskittynyt omistajuus on erityisen vahingollista PoS-lohkoketjuissa. [28] Lisää steikkaamisesta ja PoS:ista luvussa 3.4.



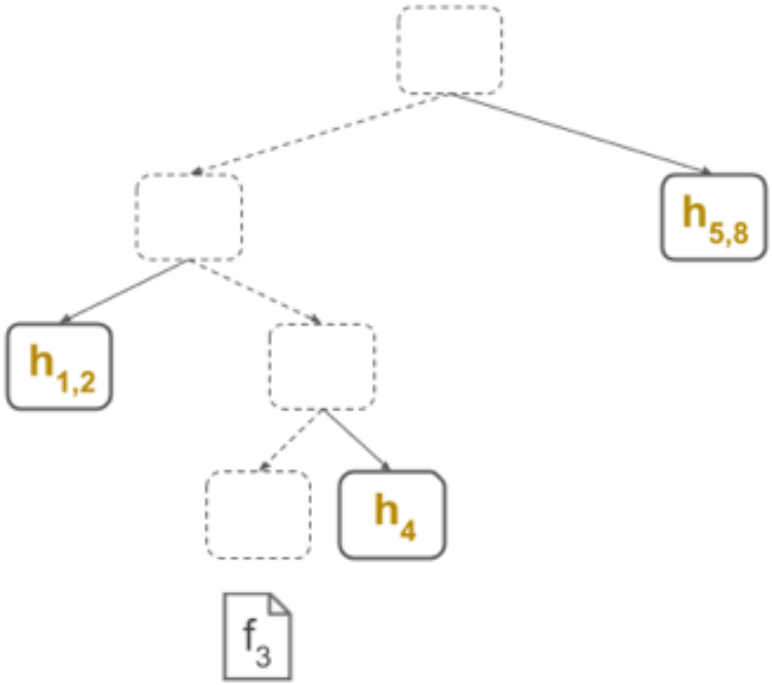
Kuva 4: Ethereumin ja sen kilpailijoiden tokenien alkuperäisiä allokaatioita [29]

Tässä luvussa käsitellään ja analysoidaan erinäisiä skaalausratkaisuja Ethereumille. Monessa näistä tekniikoista käytetään tavalla tai toisella Merkle-puita (Merkle tree). Merkle-puut ovat kryptografisiin hajautusfunktioihin perustuvia työkaluja. Lohkoketjujen tapauksessa Merkle-puissa jokaisesta transaktiosta tai tilasta tuotetaan hajautusarvo h funktiolla H. Sen jäkeen yhdistämällä kaksi h:ta kaikista hajautusarvoista luodaan yhteisiä hajautusarvoja rekursiivisesti, kunnes jäljellä on enää yksi h. Viimeiseksi muodostettua h:ta (kuvassa 5 $h_{1,8}$) kutsutaan Merkle-juureksi (Merkle root). Kuva 5 havainnollistaa tätä rakennetta.[30]



Kuva 5: Merkle-puun rakenne

Merkle-puiden avulla on mahdollista todistaa kryptografisesti esimerkiksi jonkun tilan oikeellisuus lohkossa. Tätä kutsutaan Merkle-todisteeksi (Merkle proof). Kuva 6 havainnollistaa tilannetta, jossa tila f_3 voidaan todistaa sisällytetyksi Merkle-todisteen h_4, $h_{1,2}$ ja $h_{5,8}$ kanssa. Nämä arvot ovat riittävät, jotta voidaan todentaa Merkle-juuren oikeellisuus.[30]



Kuva 6: Merkle-todisteet tilalle f_3

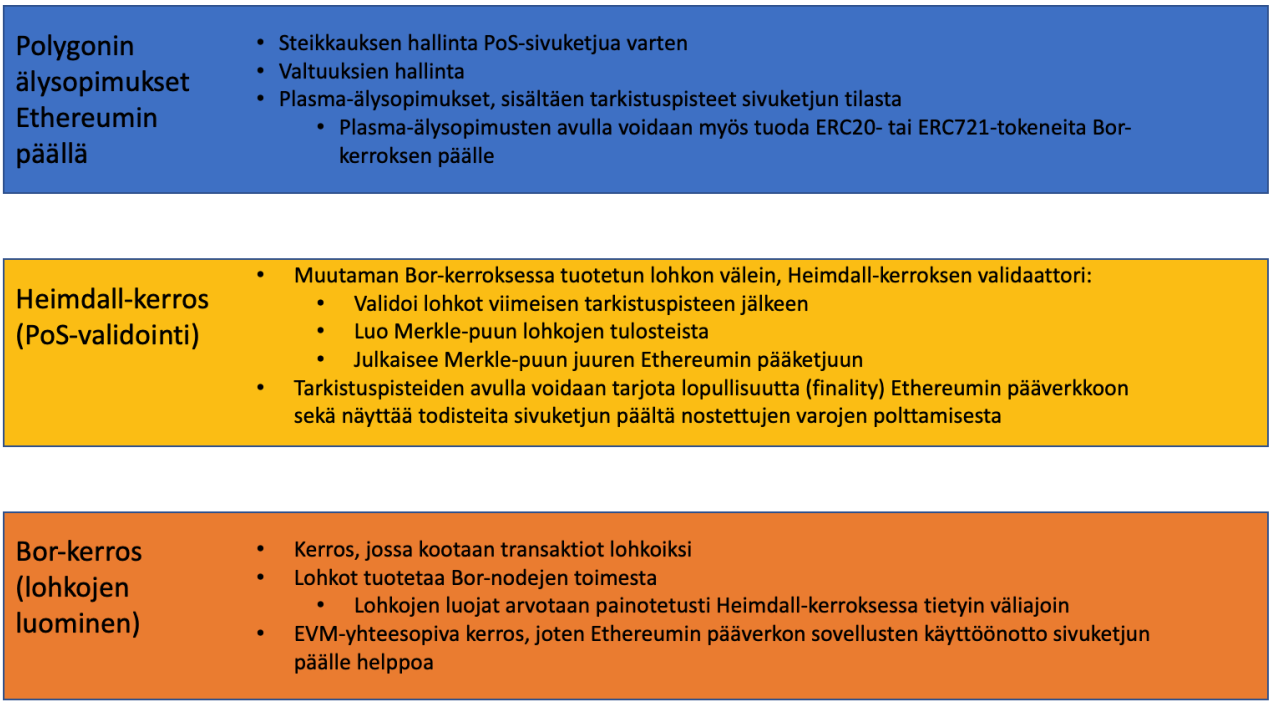
3.1 Sivuketjut ja Plasma

Sivuketju (sidechain) on erillinen oma lohkoketjunsa, joka toimii rinnakkain Ethereumin pääverkon kanssa. Se on lohkoketjun ulkopuolella tapahtuva skaalausratkaisu, koska se ei käytä pääverkkoa transaktioihinsa. Sillä on oma konsensusalgoritminsa, mikä tekee siitä keskitetymmän, eikä se peri pääverkon turvallisuusominaisuuksia. Sivuketjuissa pystytäänkin optimoimaan transaktioiden nopeutta ja kustannuksia tinkimällä turvallisuudesta, jolloin ne sopivat pienempien summien siirtoihin ja kauppoihin, DAO:jen äänestyksiin sekä moniin muihin pienemmän arvon transaktioihin. Tämä vapauttaa Ethereumin pääverkkoon lisää tilaa korkea-arvoisimmille transaktioille. Vaikka sivuketjut eivät peri pääverkon turvallisuutta, niitä yhdistää silta (bridge), jonka välityksellä varoja voidaan siirtää molempiin suuntiin. Sivuketjut ovat myös EVM-yhteensopivia, joten halutessaan käyttäjä voi ottaa käyttöön (deploy) hajautetun sovelluksensa milloin tahansa. [31], [32]

Plasma-ketjut ovat kuin sivuketjuja, mutta niitä erottaa yksi turvallisuusominaisuus: jos Plasmassa tapahtuu virhe, käyttäjät voivat turvallisesti poistua Plasma-ketjusta pääverkon päälle estäen verkkoon hyökkääjiä tekemästä pysyvää vahinkoa. Normaaleilla sivuketjuilla ei ole kyseistä ominaisuutta, joten ne eivät ole yhtä turvallisia. Plasma-ketjujen suunnittelu on kuitenkin huomattavasti vaikeampaa, jolloin niiden käyttö pienempiarvoisten sovellusten

kanssa ei ole tarpeellista. [33] Plasma-ketjut ovat myös hyviä esimerkkejä puhuttaessa aliketjuista (child chain). Niitä voidaan pinota loputtomasti päällekkäin tehden aina edellisestä Plasmasta seuraavan yläketju (parent chain), mutta kuitenkin ylimmän ketjun aina ollen Ethereumin pääverkko. Liiallinen rekursiivisuus aiheuttaa kuitenkin haasteita virhetilojen tapahtuessa, koska rekursiivinen jäljitys ylimmästä ketjusta käsin on hyvin aikaavievää. Joka tapauksessa oletusarvoisesti kaikki transaktiot suoritetaan itse aliketjussa, joten Plasma-ketjuja pidetään lohkoketjun ulkopuolella tapahtuvana skaalautuvuusratkaisuna. [33]–[35]

Esimerkiksi skaalausratkaisuihin pyrkivä Polygon tarjoaa oman hybridilohkoketjunsa, joka yhdistää sekä Plasma-ketjut että Proof-of-Stake -sivuketjun optimoidakseen nopeuden ja hajautettuneisuuden. Polygonilla on älysopimukset Ethereumin päällä Plasman lisäksi myös steikkaamisen (staking) hallintaan Proof-of-Stake -sivuketjua varten lisätäkseen sen turvallisuutta. Kuva 7 havainnollistaa Polygonin kolmekerroksista rakennetta. [36], [37]



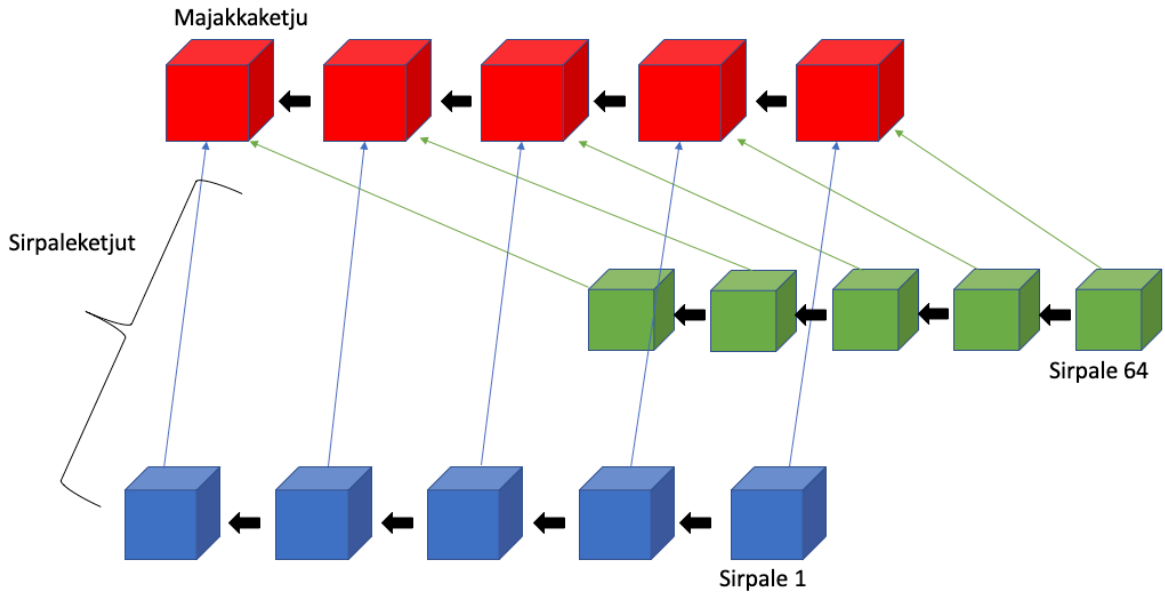
Kuva 7: Polygonin kolmekerroksinen rakenne, joka hyödyntää Ethereumin pääverkkoa, Plasma-ketjuja ja PoS-sivuketjua.

3.2 Sirpalointi

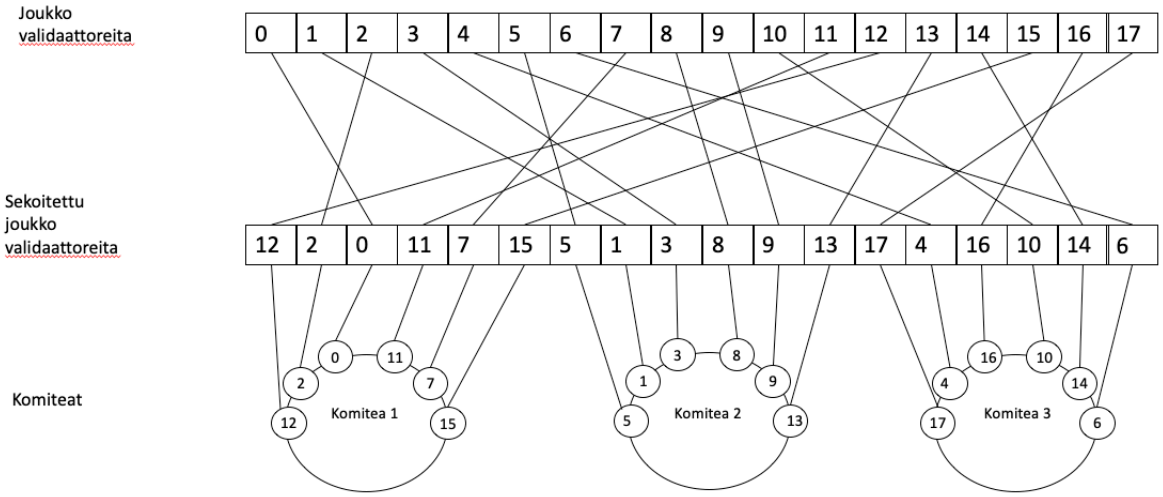
Sirpalointi (sharding) tarkoittaa tietojenkäsittelytieteen parissa tietokannan pilkkomista horisontaalisesti, jotta kuormaa saadaan jaettua. Ethereumin tapauksessa sirpalointi on uusien ketjujen, sirpaleiden (shard), luomista, mikä lisää mahdollisten transaktioiden määrää

sekunnissa (transactions per second, TPS). Sirpalointi on siis luonteeltaan lohkoketjussa tapahtuvaa skaalaamista. Ethereumiin on suunniteltu sirpaloituja lohkoketjuja, todennäköisesti vuodelle 2022, riippuen mergen eli Ethereum 1.0:n ja Ethereum 2.0:n yhdistymisen aikatauluista. Yhdistymistä käsitellään tarkemmin kappaleessa 3.4. Sirpaleita Ethereumin lohkoketjuun on suunniteltu alustavasti 64 kappaletta.[38]

Lohkoketjun jakaminen sirpaleisiin eroaa omiin erillisiin ketjuihin jakamisesta siten, että sirpaleilla on yhteinen jaettu turvallisuus ja konsensusmekaniikka, kun taas omilla erillisillä ketjuilla ei. Tämän vuoksi esimerkiksi 51%:n hyökkäykset eli hyökkäykset, joissa hyökkääjä saa haltuunsa suurimman osan nodeista ja pystyy tuottamaan virheellistä tai haitallista dataa lohkoihin, ovat huomattavasti vaikeampia sirpaloinnissa. Teknisesti jaettu turvallisuus toimii niin, että validaattorit jaetaan satunnaisesti komiteoihin (committee), jotka validoivat lohkoja. Lohkot määrätään satunnaisesti komiteoille validoitaviksi, minkä jälkeen se vahvistaa allekirjoituksella majakkaketjuun (beacon chain) validoineensa lohkon. Näin muiden validaattorien ei tarvitse vahvistaa enää lohkon sisältöä, ainoastaan allekirjoitus. Kuva 8 havainnollistaa sirpaloidun lohkoketjun rakennetta ja kuva 9 komiteoihin jakamista. Toinen ero omiin erillisiin lohkoketjuihin ja esimerkiksi Plasma-ketjuihin on sirpaloinnin tiivis kytkentä (tight coupling), joka kuvaa sitä, että yksikin virheellinen tai manipuloitu lohko yhdessäkin sirpaleessa poistetaan majakkaketjusta heti sen paljastuessa, ja koko ketju organisoituu uudelleen tämän tapahtuessa. [39]



Kuva 8: Sirpaloidun lohkoketjun rakenteen mallinnus



Kuva 9: Komiteoiden valinta arpomalla validaattorit satunnaisesti

Skaalauksen ongelmiin viitatessa nousee usein esiin lausunto skaalaustrilemmasta (the scalability trilemma). Skaalaustrilemman lausunto esittää, että ”yksinkertaisilla tekniikoilla” lohkoketju voi saavuttaa vain kaksi seuraavista kolmesta [39]:

- Skaalautuvuus: Lohkoketju voi prosessoida enemmän transaktioita kuin yksittäinen node.
- Hajautettuneisuus: Lohkoketju pystyy toimimaan ilman luottamusta pieneen keskitettyyn ryhmään. Tämän myötä ketjun ylläpidon ei tulisi vaatia liian suorituskykyisiä tietokoneita nodeiksi, jottei ylläpitävä joukko rajoitu liian pieneksi.
- Turvallisuus: Lohkoketju pystyy vastustamaan hyökkäyksiä, joissa suuri prosentuaalinen määrä nodeja yrittää tuottaa virheellisiä lohkoja. Hyökkäyksen suorittamiseen tarvittava nodejen prosentuaalinen määrä olisi ideaalitilanteessa yli 50%, mutta kaikki yli 25%:n on riittävä. Jos esim. viidellä prosentilla nodeja pystyy onnistuneesti hyökkäämään lohkoketjuun, ei ketjua voida kutsua turvalliseksi.

Näihin ”yksinkertaisiin tekniikoihin” kuuluvat perinteiset lohkoketjut, kuten Bitcoinin lohkoketju ja Ethereumin tämänhetkinen lohkoketju, koska näissä jokaisen full noden on vahvistettava jokainen transaktio. Niiltä puuttuu siis skaalautuvuus. Korkealla TPS:llä varustetut lohkoketjut eivät sen sijaan ole hajautettuja, koska ne tukeutuvat tietyn ryhmän toimesta tapahtuvaan verkon ylläpitoon. Moniketjuisissa ekosysteemeissä, joissa sovellukset

toimivat keskenään kommunikoivissa erillisissä ketjuissa, eivät ole turvallisia. Tämä johtuu siitä, että hyökkääjälle riittää yhden ketjun nodeista tarpeeksi suuren prosentuaalisen osan hallitseminen, minkä jälkeen hyökkääjä voi aiheuttaa suurta vahinkoa myös muissa ketjuissa.[39]

Sirpalointi on tekniikka, joka ratkaisee skaalaustrilemman tekemällä lohkoketjusta skaalautuvan, hajautetun ja turvallisen [39]. Virheelliset lohkot voidaan paljastaa kahdella eri tavalla:

- Todiste petoksesta (fraud proof): Lohkon sisälle voidaan muodostaa välillisiä tilan juuria (intermediate state root), jotka toimivat hajautusarvoina Merkle-puissa. Täten jos rehellinen full node käy lohkon sisältöä läpi se huomaa virheellisen välillisen tilan juuren välittömästi. Tällöin full node voi lähettää Merkle-todisteita light nodeille, jolloin light nodet voivat luottaa pelkästään otsikoiden dataan, joka niillä on jo hallussaan. Todiste petoksesta -menetelmää käytettäessä lohkoketju turvautuu kuitenkin aikaoletuksiin, mikä voi olla ongelmallista, koska jos verkko on liian hidas, nodet ovat voineet ehtiä hyväksyä lohkon ennen todisteen saapumista. [40]
- ZK-SNARK: ZK-SNARK:it ovat kryptografinen tapa todistaa tiedon oikeellisuus. Virheelliselle lohkolle ei siis voida muodostaa validia ZK-SNARK:ia. ZK-SNARK:ia käytettäessä lohkoketju ei turvaudu aikaoletuksiin. ZK-SNARK:eista lisää luvussa 3.3. [39]

Toinen sirpalointiin vaadittava turvallisuutta edistävä ominaisuus on lohkojen, joiden data ei ole saatavilla, estäminen. Datan saatavuuden varmistamiseen käytetään kahta menetelmää[41]:

- Satunnainen näytteenotto (random sampling): Jokainen node tekee satunnaisia näytteenottoja N:lle (N on esim. 30) paikkoja lohkossa, joihin se yrittää ladata dataa. Tällä pyritään todistamaan, että vähintään 50% datasta on saatavilla, ja nodejen määrän ollessa riittävän korkea, menetelmä on hyvin luotettava.
- Poistokoodaus (erasure coding): Varmistaakseen, että datan saatavuus ei jää 50-99%:iin, käytetään teknologiaa nimeltä poistokoodaus. Tämä teknologia mahdollistaa datan koodaamisen siten, että kuka tahansa, kenellä on vähintään puolet lohkon datasta, pystyy muodostamaan ja julkaisemaan loput datasta.

Sirpaloinnin tilalle ehdotetaan usein korkeamman TPS:n omaavia lohkoketjuja, mutta niiden nodeilla on mm. huomattavasti korkeammat muisti- ja suorituskykyvaatimukset tehden lohkoketjusta väistämättä keskitetymmän. Keskitettyneisyys aiheuttaa turvallisuuden kannalta suuria ongelmia, kuten sensuurin vaikeampaa tunnistamista sekä lohkojen datan varmistamista juurikin korkean TPS:n vuoksi. Myös epätoivottujen protokollamuutosten tapauksessa liian kalliit laitteistot aiheuttavat sen, että yhteisöllä ei ole todellista valtaa äänestää muutoksia vastaan, koska pieni ryhmä nodeja ylläpitäviä tahoja voi päättää, mitä versiota lohkoketjusta ne tukevat. Näin ollen sirpalointi on tällä hetkellä ainoa tosiasiallinen tapa ratkaista skaalaustrilemma. [39]

3.3 Rollupit

Rollupit (rollups) ovat eräänlainen hybridimalli lohkoketjussa tapahtuvaan skaalaamisen ja lohkoketjun ulkopuolella tapahtuvan skaalaamisen väliltä: laskenta ja tilojen varastointi tapahtuvat lohkoketjun ulkopuolella, mutta jokaista transaktiota kohden säilötään jotain dataa lohkoketjuun. Rollupit käyttävät eri tekniikoita pakatakseen dataa mahdollisimman pieneksi, jotta sen alla operoiva lohkoketju voisi toimia mahdollisimman tehokkaasti. Esimerkiksi Ethereumin päällä suoritettava ERC20 tokenin siirto maksaa n. 45 000 * polttoaineen hinta, mutta rollupin päällä tehtynä sama siirto maksaa vain alle 300 * polttoaineen hinta. [42]

Rollupit kommunikoivat alla olevan lohkoketjun kanssa sille luodun älysopimuksen kautta. Älysopimus ylläpitää rollupin tilan juurta (state root), joka on Merkle-juuri rollupin tilasta sisältäen rollupin sisällä olevan datan, kuten saldot ja sopimuskoodit. Kuka tahansa pystyy julkaisemaan erän (batch) eli kokoelman, joka sisältää tiiviisti kompressoituja transaktioita sekä rollupin vanhan ja uuden tilan juuren. Lohkoketjussa oleva älysopimus tarkistaa, että erän vanha rollupin tilan juuri on identtinen älysopimukseen tallennetun kanssa ennen rollupin tilan päivittämistä lohkoketjussa. Älysopimukseen on eroteltu myös, että mikäli erässä on transaktioita, joiden tulo- tai lähtöosoite on rollupin ulkopuolella, älysopimus alustaa kyseiset transaktiot lohkoketjun puolella. Tämä mahdollistaa nostot rollupeista sekä talletukset rollupeihin luotettavalla tavalla. Ratkaistavaksi ongelmaksi rollupeille jää se, miten pystytään todentamaan erien uusien tilojen juurten oikeellisuus. Tätä varten on kehitetty kahdenlaisia rollupeja erilaisilla teknisillä toteutuksilla: optimistiset rollupit (optimistic rollups) sekä ZK-rollupit (ZK rollups). [42] Tässä luvussa käydään läpi näiden kahden rollupin teknisiä toteutuksia. Taulukossa 1 vertaillaan niitä eri vaatimusten kannalta.

Ominaisuus	Optimistiset rollupit	ZK-rollupit
Yhden erän polttoainekustannukset	n. 40 000 * polttoaineen hinta (Vaaditaan pelkkä rollupin tilan juuren muutos.)	n. 500 000 * polttoaineen hinta (ZK-SNARK:it ovat laskentatehollisesti vaativia.)
Nostoaika	n. 1 viikko (Nostoja pitää viivästyttää, jotta mahdolliset todisteet petoksesta voidaan julkaista virheellisen noston tapauksessa.)	Seuraavan erän yhteydessä
Teknologian vaativuus	Matala	Korkea (ZK-SNARK:it ovat uusia ja matemaattisesti kompleksisia.)
Yleistettävyys	Helpompaa (Yleiskäytännöllisiä EVM-yhteensopivia rollupeja on jo Ethereumin päällä.)	Vaikeampaa (Yleiskäytännöllisten EVM-sovellusten ajamisen todistaminen ZK-SNARK:ien avulla on paljon haastavampaa. Tähän on kuitenkin kehitteillä ratkaisuja.)
Yhden transaktion polttoainekustannukset lohkoketjussa	Korkeammat	Matalammat (Transaktioissa käytettävä data, joka ei aiheuta tilan muutoksia, vaan sitä käytetään vain vahvistamiseen, voidaan jättää pois. Optimististen rollupien tulee julkaista tämä data, jos se tarvitaan tarkastaa todiste petoksesta -menetelmällä.)
Lohkoketjun ulkopuolella tapahtuvan laskennan kustannukset	Matalammat (Vaikka tarvitaan useita fullnodeja suorittamaan laskenta uudelleen.)	Korkeammat (ZK-SNARK-todistaminen yleiskäytännölliseen laskentaan voi olla todella kallista, jopa tuhansia kertoja kalliimpaa kuin laskeminen suoraan ketjussa.)

Taulukko 1: Optimististen rollupien ja ZK-rollupien vertailua [42]

3.3.1 Optimistiset rollupit

Optimistiset rollupit ovat tällä hetkellä yleiskäytännöllisempiä kuin ZK-rollupit, koska ne voidaan luoda täysin EVM-yhteensopiviksi tehden älysopimuksien ja hajautettujen sovellusten luomisesta rollupin päälle helppoa. Useimmissa optimistisissa rollupeissa, mikäli haluaa olla mukana julkaisemassa eriä lohkoketjuun, tulee tallettaa pantti lohkoketjun rollup-älysopimukseen. Tämä toimii vakuutena julkaistujen erien oikeellisuuteen – virheellisistä eristä voidaan rankaista julkaisijaa pantin menettämisen muodossa. Virheellisyyteen

optimistisissa rollupeissa käytetään todiste petoksesta -menetelmää. Kuka tahansa rollupin käyttäjistä voi luoda todisteen petoksesta käyttämällä apunaan Merkle-puita, minkä jälkeen systeemi suorittaa epäillyn transaktion uudelleen, tällä kertaa Ethereumin lohkoketjun päällä. Yleensä myös julkaistakseen todisteen petoksesta tulee tallettaa pantti, jonka voi menettää todisteen ollessa virheellinen. Tämä estää tietoverkon kuormittamisen ylimääräisillä, virheellisillä todisteilla petoksesta. Optimististen rollupien kiistatilanteiden ratkaisutavan luonteen vuoksi kaikille tietoverkon käyttäjille tulee tarjota riittävästi aikaa julkaista todisteita petoksista, minkä vuoksi varojen nostoja optimistisista rollupeista odotutetaan melko pitkään, useimmiten n. yhden viikon. [43]

3.3.2 ZK-rollupit

ZK-rollupeja eli Zero Knowledge -rollupeja varten on tärkeää ymmärtää ZK-SNARK:ien toimintaa. ZK-SNARK-lyhenne tulee sanoista "zero knowledge succinct arguments of knowledge", joka tarkoittaa ytimekkäitä tiedon argumentteja nollatietämyksellä. Ytimekkyydellä tarkoitetaan sitä, että vahvistamisen tulisi tapahtua suorittamalla koko laskentaprosessi kuitenkaan suorittamatta jokaista laskutoimitusta. Esimerkiksi satunnainen näytteenotto ja Merkle-juurien laskeminen ei toimi tähän tarkoitukseen, koska suuren datamäärän ja kohtuullisen kokoisen näytteen kanssa pienet, kuten vain yhden bitin muutokset, jäisivät lähes aina huomaamatta. Tämän ratkaistakseen ZK-SNARK:it käyttävät polynomisia sitoumuksia (polynomial commitments), jotka tukeutuvat uudehkoon kompleksiseen matematiikkaan, kuten Kate-sitoumuksiin (Kate commitments) ja elliptisten käyrien paritukseen (elliptic curve pairings) tai FRI:hin (Fast RS IOPP, RS=Reed-Solomon, IOPP=Interactive Oracle Proofs of Proximity). Polynomiset sitoumukset ovat yksinkertaistettuna tapa suorittaa hajautusalgoritmi polynomille niin, että polynomien välisiä funktioita voidaan tarkastaa polynomien hajautusarvojen osalta. Näin ollen hajautusarvoille voidaan tehdä matemaattisia tarkistuksia satunnaisilla arvoilla nojaten Schwartz-Zippelin lemmaan, joka on seuraavanlainen: [44]

- Olkoon F kenttä. Olkoon $f(x_1, x_2, ..., x_n)$ polynomi, jonka aste on d ja oletetaan, että f ei ole identtinen nollapolynomin kanssa. Olkoon S F:n rajallinen alijoukko. Olkoon r_1, r_2, ..., r_n tasaisesti ja satunnaisesti valittu alijoukosta S. Tällöin todennäköisyys sille, että $f(r_1, r_2, ..., r_n) = 0$ on $\leq d/|S|$.

Lemman avulla voidaan todeta, että alijoukon S ollessa riittävän suuri, on erittäin todennäköistä, että satunnaisesti valitulla arvolla r oikeellisen tuloksen tuottava polynomi on oikeellinen. ZK-SNARK:eissa voidaan lisäksi välttää satunnaisen arvon valitseminen valitsemalla esimerkiksi laskennan Merkle-juuren, jolloin todistaja ei voi valita suotuisia arvoja virheelliselle polynomille. Polynomien kasvaessa suureksi ja r:ksi valikoituessa suuri kokonaisluku, on ZK-SNARK:eissa tapana, kuten usein muutenkin kryptografiassa, valita jokin alkuluku p moduloksi ja käsitellä polynomia tämän jakojäännosten perusteella: [45]

- x + y => (x + y) % p
- x * y => (x * y) % p
- jne.

ZK-rollupit toimivat siis niin, että siinä missä optimistinen rollup julkaisee rollupin uuden Merkle-juuren, ZK-rollup julkaisee kryptografisen todisteen, ZK-SNARK:in, josta voidaan todella nopeasti varmistaa julkaistun erän oikeellisuus. Näin ollen esimerkiksi nostot voidaan varmistaa heti seuraavan erän julkaisun yhteydessä ilman vaadittavia odotusaikoja. ZK-rollupit eivät ole kuitenkaan ylivertaisia verrattuna optimistisiin rollupeihin, vaan niilläkin on omat haasteensa. Esimerkiksi nodejen, jotka laskevat ZK-SNARK:ien todisteita, tulee olla laskentatehollisesti todella tehokkaita laskennan kompleksisuuden vuoksi, mikä rajaa käyttäjien mahdollisuutta ylläpitää nodeja. Myös alla piilevän teknologian kompleksisuuden vuoksi EVM-yhteensopivaa ZK-rollupia on todella hankalaa skaalata yleiskäytännöllisille sovelluksille ilman, että se vaatisi koko sovelluksen logiikan uudelleenkirjoittamista. Tässä on tosin tapahtunut viime aikoina kehitystä mm. ZKSyncissä (yritys Matter Labsin kehittämässä ZK-rollup-ratkaisussa [46]), joka on osoittanut saattavansa pystyä julkaisemaan Ethereumin päälle EVM-yhteensopivan ZK-rollupin lähitulevaisuudessa. [43]

3.4 Proof-of-Stake

Ethereum käyttää tällä hetkellä Bitcoinin tapaan Proof-of-Work eli PoW-konsensusmekanismia, jonka avulla vertaisverkko voi olla yhteisymmärryksessä mm. saldoista ja transaktioiden järjestyksestä sekä tehdä lohkoketjuun hyökkääminen tai manipulointi mahdollisimman vaikeaksi. Ethereumin Proof-of-Work-protokolla Ethash toimii antamalla louhijoille, eli työtä tekeville verkon ylläpitäjille, tietojoukkoja, josta louhijat matemaattisen funktion avulla pyrkivät kokeilemalla saamaan lohkon järjestysnumeron.

Oikean järjestysnumeron ensimmäisenä saanut louhija saa kaksi etheriä sekä lohkon transaktioihin käytetyt transaktiomaksut luoden kannustimen tekemään työtä ja näin osallistumaan verkon ylläpitämiseen. Muiden louhijoiden on helppo tarkistaa lohkon oikeellisuus sen hajautusarvosta. PoW-konsensuksessa suurimpana turvallisuusriskinä ovat 51%:n hyökkäykset.[47]

Ethereum on kuitenkin vaihtamassa konsensusmekanismikseen Proof-of-Stakea eli steikkaamiseen perustuvaa konsensusta. Konsensusmekanismin vaihto tapahtuu, kun tämänhetkinen Ethereum 1.0 sekä joulukuusta 2020 käytössä ollut PoS-konsensusmekanismin omaava Ethereum 2.0 yhdistyvät. Tätä yhdistymistä kutsutaan mergeksi ja sen arvioidaan tapahtuvan vuoden 2022 aikana. [48], [49]

Steikkaaminen tarkoittaa varojen, Ethereumin tapauksessa etherin, lukitsemista full nodeen, joka toimii validaattorina verkossa. Steikatut varat toimivat sekä panttina, jotta väärinkäytöksistä ja virheellisestä validoinnista voidaan rankaista, että tuottoa tuottavana omaisuuseränä, koska steikkaajat palkitaan oikeellisesta validointityöstään. Ethereumissa PoS-konsensukselle on luotu ns. lopullisuusprotokolla, Casper, joka määrittää tietyin väliajoin lohkojen lopullisuutta. Tähän vaaditaan Casperin mukaan 2/3 validaattoreista. Jos validaattori yrittää kumota lopullista lohkoa myöhemmin, menettää se kaikki steikatut varansa. Proof-of-Staken edut Proof-of-Workiin nähden ovat selvät niin skaalautuvuden kuin käytännöllisyyden puolesta: [48], [50]

- Proof-of-Staken validaattorit eivät kuluta läheskään niin paljoa sähköä kuin Proof-of-Workin louhijat, eikä validointiin osallistuminen vaadi kovin kallista laitteistoa.
    - Sähkönkulutuksen vähentymisen myötä myös tarve lisätä uutta valuuttaa markkinoille pienenee.
- Vähennetty keskitettyneisyyden riski sen myötä, että 10-kertainen steikkausmäärä aiheuttaa 10-kertaisen tuoton, kun taas PoW:issa suuremmalla panostuksella saa suhteessa tehokkaammat laitteet ja näin ollen paremman tuoton.
    - Myös nodejen määrä kasvaa, Ethereum 2.0:ssa on jo yli 250 000 aktiivista validaattoria. [51]
- PoS-konsensus tarjoaa turvallisemman ympäristön sirpaloinnille, koska Ethereumin luodessa useita lohkoja yhtaikaa horisontaalisesti, PoW-konsensuksella vaadittava

työmäärä hyökkäyksessä sirpaletta kohtaan olisi väistämättä matalampi kuin koko ketjua kohtaan.

Ryhtyäkseen Ethereum 2.0:n validaattoriksi vaaditaan 32:n etherin steikkaus. Tämä on tarkasteluhetkellä (13.12.2021) arvoltaan yli 120 000 dollaria [52], mikä rajaa mahdollisia steikkaajia pois. Tätä ongelmaa rajatakseen ja sitä kautta keskitettyneisyyden estämistä varten on perustettu useita hajautettuja steikkauspalveluita, kuten Rocket Pool ja Lido. Tällaiset toimijat mahdollistavat ihmisten varojen yhdistämisen ja sitä kautta steikkaamiseen osallistumisen sekä siitä syntyvien tulovirtojen saavutettavuuden. [53], [54]

4 Yhteenveto ja johtopäätökset

Ethereumin suuri suosio on nostanut sen käytön kustannuksia ja tätä varten on jouduttu kehittämään erinäisiä skaalausratkaisuja. Skaalausta on lähestytty useasta eri näkökulmasta ja jokaisella näistä on omat hyvät ja huonot puolensa. Skaalaamiseen tullaan käyttämään näitä kaikkia ratkaisuja, jokaista omiin tarkoituksiinsa. Osa esitellyistä skaalausratkaisuista ei ole vielä teknisesti sillä tasolla, että ne voitaisiin ottaa käyttöön, mutta edistystä tapahtuu jatkuvasti.

Sirpalointi on ainoa tämänhetkisistä skaalausratkaisuista, jonka avulla pystytään kasvattamaan pohjakerroksen (base layer) eli Ethereumin lohkoketjun skaalautuvuutta luopumatta yhdestäkään skaalaustrilemman osa-alueesta. Sirpaloinnin tekninen toteutus vaatii kuitenkin paljon kehitystä ennen kuin se saadaan integroitua Ethereumiin, joten skaalausratkaisut ovat tarpeen jo ennen sitä. Sirpaloinnilla ei myöskään pystytä skaalaamaan lohkoketjuja loputtomasti todistusvaatimusten vuoksi, joten myös tulevaisuudessa muille ratkaisuille on paikkansa.

Matalan turvallisuusvaatimusten omaaviin transaktioihin voidaan käyttää sivuketjuja tai Plasmaa, koska näillä voidaan saavuttaa nopeat ja halvat transaktiot. Esimerkiksi konsoli- ja tietokonepelien mikromaksut voisivat huoletta tapahtua näissä vaihtoehdoissa, jotta lukuisat transaktiot maksaisivat käyttäjälle vain senttien murto-osia, eikä näin ollen karsi jokapäiväisiä käyttäjiä pois.

Vaikka rollupien kehittäminen ja ylläpitäminen tapahtuisikin keskitetysti tai keskitetymmin kuin lohkoketjut, niiden pohjakerroksena toimii Ethereumin lohkoketju, joka on hajautettu ja turvallinen. Näin ollen rollupien keskitettyyn rakenteeseen voidaan luottaa, koska matematiikan avulla perustelemalla se pystyy osoittamaan olevansa sensuurivapaa hajautetun pohjakerroksen päällä. Tämän vuoksi rollupit tarjoavat enemmän turvallisuutta, kuin esimerkiksi sivuketjut. [55]

Sivuketjut, Plasma ja rollupit voivat kaikki olla tulevaisuudessakin olemassa skaalaamassa Ethereumia sirpaloinnin rinnalla, jokaisen tarjotessa omat vahvuutensa. Vaikka sivuketjut ovat tällä hetkellä kaikkein valmiimpia ratkaisuja, näyttää tulevaisuus enemmän rollup-keskeiseltä näiden teknisen toteutuksen vuoksi. Rollupeista optimistiset rollupit ovat toteukseltaan edellä, mutta pidemmällä aikavälillä ZK-SNARK:ien kehittyessä, tulevat sekä rollupit että sirpalointi keskittymään enemmän tämän teknologian ympärille. [56]

Lähteet

[1] "Ethereum Whitepaper" https://ethereum.org/en/whitepaper/ (haettu 17.10.2021).

[2] Jeff Benson "War Over Ethereum Gas Fees and Usability Continues" Decrypt https://decrypt.co/86640/war-ethereum-gas-fees-usability-continues (haettu 14.12.2021).

[3] D. Yaga, P. Mell, N. Roby, ja K. Scarfone, "Blockchain Technology Overview" NIST, Lokakuu 2018, doi: 10.6028/NIST.IR.8202.

[4] S. Sifis Lagouvardos, Neville Grech, Ilias Tsatiris, ja Yannis Smaragdakis, "Precise Static Modeling of Ethereum ``Memory''" Marraskuu 2020, doi: 10.1145/3428258.

[5] K. Bhargavan *ym.*, "Formal verification of smart contracts: Short paper," *PLAS 2016 - Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, co-located with CCS 2016*, ss. 91–96, Lokakuu 2016, doi: 10.1145/2993600.2993611.

[6] Tai "The Account Nonce in Ethereum Explained" Coinmonks Medium https://medium.com/coinmonks/the-account-nonce-in-ethereum-explained-c087bd4a3c29 (haettu 18.10.2021).

[7] Ethereum Homestead 0.1 documentation "Account Types, Gas, and Transactions" https://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html (haettu 17.10.2021).

[8] ethereumbook Github "ethereumbook/07smart-contracts-solidity.asciidoc at develop" https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc#what-is-a-smart-contract (haettu 24.10.2021).

[9] EthHub "What is Ethereum?" https://docs.ethhub.io/ethereum-basics/what-is-ethereum/#what-are-smart-contracts-and-decentralized-applications (haettu 24.10.2021).

[10] Ethereum.org "Introduction to dapps" https://ethereum.org/en/developers/docs/dapps/ (haettu 24.10.2021).

[11] Dimitar Bogdanov (Kesäkuu 2021) "What are dApps: A 2021 guide to decentralized applications" LimeChain https://limechain.tech/blog/what-are-dapps-the-2021-guide/ (haettu 24.10.2021).

[12] OpenZeppelin Docs "Tokens" https://docs.openzeppelin.com/contracts/3.x/tokens (haettu 24.10.2021).

[13] OpenZeppelin Docs "ERC20" https://docs.openzeppelin.com/contracts/3.x/erc20 (haettu 24.10.2021).

[14] Ethereum.org "Decentralized finance (DeFi)" https://ethereum.org/en/defi/ (haettu 24.10.2021).

[15] OpenZeppelin Docs "ERC721" https://docs.openzeppelin.com/contracts/3.x/erc721 (haettu 24.10.2021).

[16] Ethereum.org "Non-fungible tokens (NFT)" https://ethereum.org/en/nft/ (haettu 24.10.2021).

[17] OpenZeppelin Docs “ERC1155” https://docs.openzeppelin.com/contracts/3.x/erc1155 (haettu 24.10.2021).

[18] Ethereum.org “Nodes and clients” https://ethereum.org/en/developers/docs/nodes-and-clients/ (haettu 24.10.2021).

[19] Ethereum.org “Scaling” https://ethereum.org/en/developers/docs/scaling/ (haettu 24.10.2021).

[20] Etherscan “Ethereum Node Tracker” https://etherscan.io/nodetracker (haettu 29.11.2021).

[21] DefiLlama “Binance TVL” https://defillama.com/chain/Binance (haettu 29.11.2021).

[22] BscScan “Binance Validators” https://bscscan.com/validators (haettu 29.11.2021).

[23] Everett Muzzy ja Mally Anderson “Measuring Blockchain Decentralization” ConsenSys Research, ConsenSys https://consensys.net/research/measuring-blockchain-decentralization/ (haettu 29.11.2021).

[24] DefiLlama “Solana TVL” https://defillama.com/chain/Solana (haettu 29.11.2021).

[25] Solana Beach “Dashboard” https://solanabeach.io/ (haettu 29.11.2021).

[26] CoinGecko “Solana (SOL)” https://www.coingecko.com/en/coins/solana (haettu 29.11.2021).

[27] Staking Rewards “Solana (SOL) Interest Calculator and Current Rates” https://www.stakingrewards.com/earn/solana/ (haettu 29.11.2021).

[28] Greenchic (Marraskuu 2021) “Solana is a buzzing popular Blockchain, however its criticized for being very centralized.” Publish0x https://www.publish0x.com/investing-and-trading/solana-is-a-buzzing-popular-blockchain-however-its-criticize-xqmwvly (haettu 29.11.2021).

[29] Messari “Cryptoassets Research Reports” https://messari.io/research (haettu 29.11.2021).

[30] Alin Tomescu (Joulukuu 2020) “What is a Merkle Tree?” Decentralized Thoughts https://decentralizedthoughts.github.io/2020-12-22-what-is-a-merkle-tree/ (haettu 6.12.2021).

[31] EthHub “Sidechains” https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/sidechains/ (haettu 25.10.2021).

[32] Ethereum.org “Sidechains” https://ethereum.org/en/developers/docs/scaling/sidechains/ (haettu 25.10.2021).

[33] Vitalik Buterin (Kesäkuu 2019) “Sidechains vs Plasma vs Sharding.” https://vitalik.ca/general/2019/06/12/plasma_vs_sharding.html (haettu 25.10.2021).

[34] S. Dziembowski, G. Fabiański, S. Faust, ja S. Riahi, “Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma”, University of Warsaw, 2020.

[35] G. Kaur ja C. Gandhi, “SCALABILITY IN BLOCKCHAIN: CHALLENGES AND SOLUTIONS” *Blockchain Implementation for Internet of Things Applications Energy effiecient WSN View project Wireless Sensor Networks Lab View project*, ss. 373–406, 2020, doi: 10.1016/b978-0-12-819816-2.00005-8.

[36] Polygon Technology “Documentation.” https://docs.polygon.technology/ (haettu 25.10.2021).

[37] Polygon “Ethereum’s Internet of Blockchains.” https://polygon.technology/ (haettu 25.10.2021).

[38] Ethereum.org “Shard chains” https://ethereum.org/en/eth2/shard-chains/ (haettu 7.12.2021).

[39] Vitalik Buterin (Huhtikuu 2021) “Why sharding is great: demystifying the technical properties.” https://vitalik.ca/general/2021/04/07/sharding.html (haettu 7.12.2021).

[40] M. Al-Bassam, A. Sonnino, and V. Buterin, “Fraud and Data Availability Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities”, University College London, Ethereum Research, Toukokuu 2019.

[41] Vitalik Buterin “An explanation of the sharding + DAS proposal” HackMD https://hackmd.io/@vbuterin/sharding_proposal#ELI5-data-availability-sampling (haettu 11.12.2021).

[42] Vitalik Buterin (Tammikuu 2021) “An Incomplete Guide to Rollups.” https://vitalik.ca/general/2021/01/05/rollup.html (haettu 12.12.2021).

[43] Jakub (Helmikuu 2021) “Rollups – The Ultimate Ethereum Scaling Solution” Finematics https://finematics.com/rollups-explained/ (haettu 12.12.2021).

[44] Patrick Corn ja Jimin “Schwartz-Zippel Lemma” KhimBrilliant Math & Science Wiki https://brilliant.org/wiki/schwartz-zippel-lemma/ (haettu 29.1.2022).

[45] Vitalik Buterin (tammikuu 2021) “An approximate introduction to how zk-SNARKs are possible.” https://vitalik.ca/general/2021/01/26/snarks.html (haettu 13.12.2021).

[46] ZKSync “Rely on math, not validators.” https://zksync.io/ (haettu 13.12.2021).

[47] Ethereum.org “Proof-of-work (PoW).” https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/ (haettu 13.12.2021).

[48] Ethereum.org “Proof-of-stake (PoS)” https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ haettu 13.12.2021).

[49] Ethereum.org “The Beacon Chain” https://ethereum.org/en/eth2/beacon-chain/ (haettu 13.12.2021).

[50] Vitalik Buterin (Joulukuu 2017) “Proof of Stake FAQ.” https://vitalik.ca/general/2017/12/31/pos_faq.html (haettu 13.12.2021).

[51] beaconcha.in (2021) “Ethereum 2.0 Beacon Chain (Phase 0) Block Chain Explorer - Index” https://beaconcha.in/ (haettu 13.12.2021).

[52] CoinGecko “Ethereum (ETH)” https://www.coingecko.com/en/coins/ethereum (haettu 13.12.2021).

[53] Lido Finance “FAQ” https://lido.fi/faq (haettu 13.12.2021).

[54] David Rugendyke (Tammikuu 2021) “Rocket Pool — Staking Protocol Part 1” Rocket Pool Medium https://medium.com/rocket-pool/rocket-pool-staking-protocol-part-1-8be4859e5fbd (haettu 13.12.2021).

[55] Vitalik Buterin (Joulukuu 2021) “Endgame.” https://vitalik.ca/general/2021/12/06/endgame.html (haettu 14.12.2021).

[56] Vitalik Buterin (Lokakuu 2020) “A rollup-centric ethereum roadmap” Fellowship of Ethereum Magicians https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698 (haettu 14.12.2021).