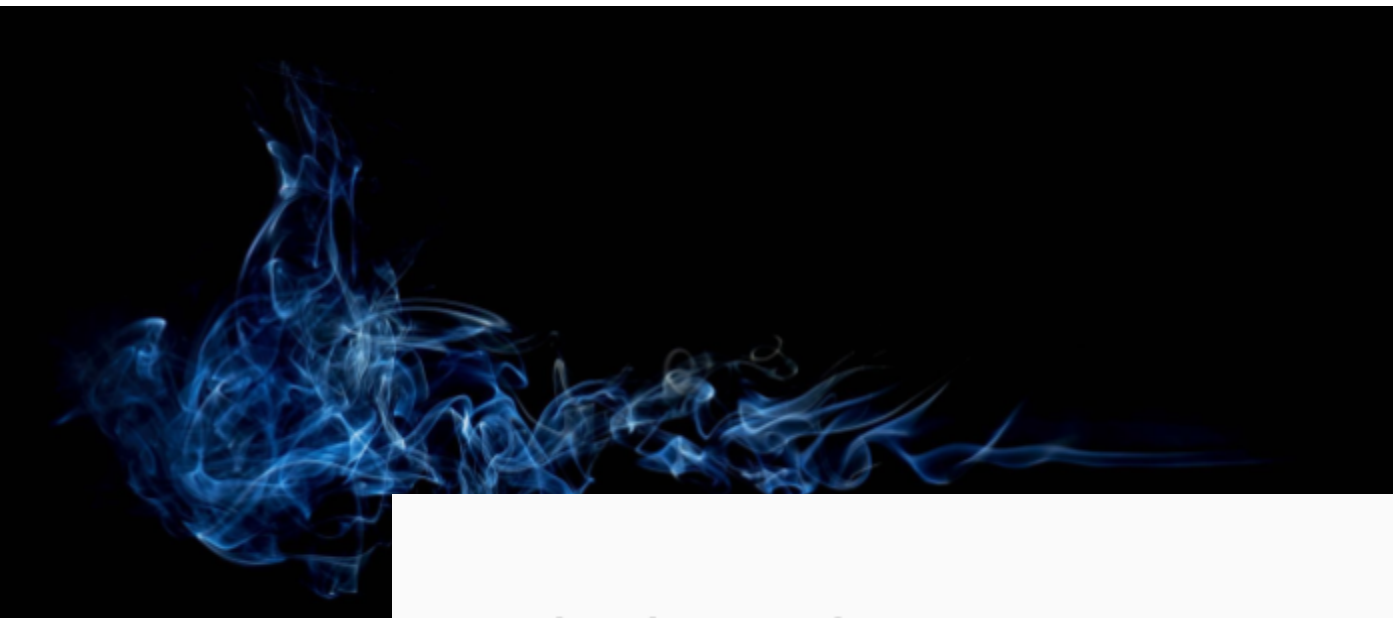




Coinmotion Research

Tutkimuksia, selvityksiä ja julkaisuja 1 • 2022

Ethereumin tulevaisuus

Beacon Chain, The Merge ja shard chains

– Suppea näkökulma

Thomas Brand
Head of Institutions
institutions@coinmotion.com

31. maaliskuuta 2022



Sisällysluettelo

<u>Yhteenveto</u>	3
<u>Johdanto: Ethereumin joukkorahoitus ja käynnistäminen</u>	5
<u>Työntodisteesta irtautuminen</u>	9
<u>Ethereumin neljä kehitysvaihetta</u>	12
<u>Tyyneys kulman takan? – Lyhyt johdanto Serenity-vaiheeseen</u>	17
<u>Kiln-testiverkko siirrettiin onnistuneesti varantodisteeseen</u>	21
<u>ETH2-panttaamisen suosio jatkaa kasvuaan</u>	25
<u>Miten tästä eteenpäin?</u>	32

TL;DR: Yhteenveto

Rakentuuko tulevaisuuden finanssiala Ethereumin, maailman toistaiseksi suurimman avoimen lähdekoodin julkisen lohkoketjun, varaan? Ainakin osa finanssialan toimijoista näyttää erilaisten kokeilujen perusteella uskovan siihen, että Ethereumin päällä kannattaa kokeilla erilaisia asioita, kuten esimerkiksi joukkovelkakirjojen liikkeeseenlaskua. Tämä siitä huolimatta, että Ethereumin siirtokulut ovat nousseet merkittävästi vuoden 2021 alusta alkaen ja Ethereumissa on toteutettu lukemattomia hankaliksi miellettyjä ohjelmistopäivityksiä jopa protokollatasolle asti. Tämä on ainakin osittain edesauttanut Ethereumin kanssa kilpailevien L1-ketjujen syntyä, kasvua ja kehitystä. Nyt lähes kaikki suuret päivityskokonaisuudet on saatu tehtyä, joten viimeistään viime vuonna kehittämisen painopiste siirtyi vahvasti yrityksiin skaalata verkkoa. *Mitä parempi arvoverkko, sitä enemmän arvokasta vaihtoa.*

Ethereum toimii vielä tällä hetkellä energiasyöppönä pidetyn työntodistekonsensuksen varassa (*PoW, Proof of Work*). Halu siirtyä hallitusti (mutta riittävän nopeasti) pois työntodisteesta energia- ja laskentatehokkaampana pidetyn varantodistukseen (*PoS, Proof of Stake*) on vahvistunut kuluneiden vuosien aikana. Ethereumin pääketju on määrä sulauttaa *Beacon Chainiin* eli Ethereumin PoS-rinnakkaisketjuun vielä kuluvan vuoden aikana.

Ethereum saavutti suuren virstanpylvään maaliskuun puolivälissä, kun *The Merge* -nimellä kulkeva ohjelmistopäivitys saatiin toteutettua Ethereumin julkisessa Kiln-testiverkossa. Kyse oli "vain" testauksesta, mutta samalla saatiin varmuus siitä, että sulautuminen on mahdollista toteuttaa. Sulautuminen ei ollut mutkaton, mutta satojen miljardien arvoisen hajautetun arvoverkon muutoksia toteuttaa tuhansia ihmisiä. Äärimmilleen hajautettu työnjako, erikoistuminen ja mahdollisuus päästä mukaan ilman sitoumuksia varmistavat, että virheitä etsitään, löydetään ja korjataan ilman keskusjohtoa.

Sijoittajat äänestävät jatkuvasti lompakollaan. Testisulautumisen onnistuminen vaikutti myönteisesti ETH-tokenin hintaan ja kasvatti intoa lukita ETH:ta Beacon Chainin ETH2-talletussopimukseen joskus tulevaisuudessa maksettavan "steikkaustulon" ansaitsemiseksi. Lohkoketjudata paljastaa, että lukitun ETH:n määrä on kasvanut merkittävästi testisulautumisen jälkeen ja ETH:n hintakin on noussut kuukauden aikana myönteisesti.

Onnistunut testisulautuminen on myönteistä myös jo ansaittujen erilaisten ETH2-tokeneiden likviditeetin kannalta, koska itse ETH2-talletussopimukseen lukittua ETH:ta ja tulevaisuudessa maksettavia steikkaustuloja ei voi vielä käyttää. Niiden vapauttamisen aikataulu on vielä toistaiseksi epävarma (vaihtoehtoiskustannukset tärkeä ymmärtää!).

Mielestäni on itsestään selvää, että ETH:n olemus on muuttumassa. Testisulautuminen vauhdittaa muutosta, jossa ETH saattaa muuttua sijoittajien silmissä eräänlaiseksi *haltijaomaisuusmaiseksi ikuiseksi saamistodistukseksi*. Se voi tuottaa *steikkattuna* (tai lainattuna) ETH-määristä kassavirtaa. En pidä myöskään poissuljettuna sitä, että tulevaisuudessa ETH:n ajatellaan olevan eräänlainen Ethereum-ekosysteemin vähäriskinen varanto-omaisuuserä.

Sulautuminen onnistui testissä, koska testiverkossa liiketoimia vahvistetaan, isketään lohkoihin ja liitetään testiketjuun tälläkin hetkellä. Verkon tehokkuutta, tapahtumakäsittelyn nopeutta ja siirtokuluja alentavat protokollatason skaalausratkaisuja on hankala toteuttaa, mutta ne voivat toisaalta onnistuessaan luoda paljon nostetta ja vetää myönteisen kierteen ansiosta mukaan muun muassa ohjelmistokehittäjiä, sijoittajia ja yrittäjiä.

Yleisesti ottaen minusta tuntuu joskus siltä, että Ethereumin suurimmat haasteet johtuvat tasapainoilusta kahden vision välillä: puhdas ja yksinkertainen lohkoketju, jossa arvostetaan turvallisuutta ja yksinkertaisuutta, ja erittäin tehokas ja toimiva alusta kehittyneiden sovellusten rakentamiseen. – –

Minun unelmani on pyrkiä saavuttamaan molemmat visiot samanaikaisesti: peruskerros – – ja tehokas käyttäjäystävällinen kehittyneiden sovellusten ekosysteemi, jonka keskiössä ovat toisen kerroksen protokollat. – –

Nykyään on paljon asioita, joita emme voi muuttaa, mutta monia asioita voimme edelleen muuttaa, ja sekä toiminnallisuuden ja yksinkertaisuuden parantamiseen on vielä varaa. Joskus polku on mutkitteleva: meidän on ensin kasvatettava monimutkaisuutta, jotta voimme tehdä sirpaloittamisen mahdolliseksi, mikä puolestaan mahdollistaa runsaan toisen tason skaalautuvuuden.

– Vitalik Buterin | *The roads not taken* (2022)

Johdanto: Ethereumin joukkorahoitus ja käynnistäminen

“Ethereum 1.0:aa voi pitää prototyyppinä. Meidän oli julkaistava jotain, jonka tiesimme olevan skaalautumaton. Halusimme todistaa, että desentralisoituja sovelluksia on mahdollista rakentaa.”

– Vitalik Buterin¹

Vitalik Buterin julkaisi yleiskäyttöiseksi suunnitellun Ethereum-lohkoketjun² teknisen kuvauksen³ tammikuussa 2014 ja kertoi tavoitteistaan myös bitcoinaajien suosimalla *bitcointalk*-keskustelufoorumilla tammikuun lopussa.⁴

Ethereumin teknisessä kuvauksessa Buterin kuvasi Ethereumin toteutustapaa, arkkitehtuuria ja erilaisia käyttötapauksia. Esitettyjä käyttötapauksia olivat muun muassa ERC20-tyyppiset tokenit, algoritmiset vakaakolikot⁵, johdannaiset, hajautettu tiedostojen tallennus ja laskenta, DAO:t eli desentralisoidut autonomiset organisaatiot, oraakkelit ja ennustemarkkinat.⁶

Ethereumin ETH-liikkeeseenlasku⁷ järjestettiin bitcoin-karhumarkkinan keskellä loppukesästä 2014.⁸ Vitalik Buterin julkaisi liikkeeseenlaskusta tarkempaa tietoa Ethereum Foundationin blogissa.⁹

Bitcoinin hinta pyöri tuolloin 600 USD:n molemmin puolin. Liikkeeseenlaskun alkumetreillä yhdellä BTC:llä sai 2 000 ETH:ta, jonka jälkeen yhdellä BTC:llä “merkittävän” ETH:n määrä laski ennalta määrätyllä tavalla siten, että lopulta

¹ ConsenSys 2019: [30 Quotes that Defined a Momentous Ethereal Summit](#). ConsenSys Blog; ks. myös Kyle Torpey 2016: [Vitalik Buterin on His Long-Term Goals for Ethereum](#). Bitcoin Magazine.

² Hyvinä johdantona Ethereumiin, ks. Chris Dannen 2017: *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. New York, NY: Apress; Andreas M. Antonopoulos & Gavin Wood 2019: *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA: O'Reilly Media.

³ Vitalik Buterin 2022 [2014]: [A Next-Generation Smart Contract and Decentralized Application Platform](#). Buterin julkaisi teknisen kuvauksen [ensimmäisen version](#) jo marraskuussa 2013 työskenneltyään Omni-lohkoketjuhankkeen (ex-Mastercoin) parissa, ks. [arkistoitu versio](#) Ethereumin teknisestä kuvauksesta ja [ethereum.org](#)-verkkosoitteen [rekisteriöintiajankohta](#). Enemmän Ethereumin esihistoriasta, ks. Vitalik Buterin 2017: [A Prehistory of the Ethereum Protocol](#). Ks. myös Victoria van Eyk 2014 [2021]: [Ethereum Launches Own 'Ether' Coin, With Millions Already Sold](#).

⁴ Buterinin julkaisemaan viestiketjuun on tähän päivään mennessä kirjoitettu lähes 26 000 kommenttia. Vitalik Buterin 2014: [\[ANN\] Ethereum: Welcome to the Beginning](#). Bitcoin Forum.

⁵ Tunnetaan englanniksi nimellä *stablecoin*.

⁶ Vitalik 2022: [Twitter](#).

⁷ Tunnetaan englanniksi nimellä *ICO*, *Initial Coin Offering*, ks. Finanssivalvonta 2019: [Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu?](#). Lisätietoja ICO:ista ja niiden dynamiikasta: Anca Mirela Toma & Paola Cerchiello 2020: [Initial Coin Offerings: Risk or Opportunity?](#). *Frontier in Artificial Intelligence* 16.4.2020; Paul P. Momtaz 2020: [Initial Coin Offerings](#). *PLOS One* 21.5.2020. ETH tai Ξ on Ethereum-tietojenkäsittely-ympäristön oma natiivi token.

⁸ Academy 2020: [Ethereum: The Greatest ICO in History](#). Ethereumin roolista myöhempien vuosien ICO-boomissa, ks. Jason Rowley 2017: [How Ethereum became the platform of choice for ICO'd digital assets](#). TechCrunch; Cryptopedia Staff 2022: [Ethereum and the ICO Boom](#).

⁹ Vitalik Buterin 2014: [Launching the Ether Sale](#). Ethereum Foundation Blog.

yhdellä BTC:llä sai 1 337 ETH:ta. Yhden ETH:n laskennallinen hinta oli ICO-merkinnän alussa noin 0,31 USD.¹⁰

Ethereumin 22. heinäkuuta 2014 käynnistynyt liikkeeseenlasku oli menestys: yli seitsemän miljoonaa ETH-yksikköä ennakkomyytiin vain 12 tunnin kuluessa (~2,2 miljoonaa EUR) liikkeeseenlaskun julkaisemisesta ja kahden viikon aikana bitcoinaajille ennakkomyytiin yhteensä yli 60 miljoonaa ETH-yksikköä.¹¹

Bitcoinaajille ennakkoon myyty ETH vastasi noin 83 %:ia kokonaistarjonnasta, joka vuoden 2015 Ethereumin käynnistymisen yhteydessä luovutettiin “merkitsijöille”.¹² Buterinin mukaan noin puolet nykyisin olemassa olevasta ETH:sta myytiin tässä yhteydessä.

Lisäksi noin 12 miljoonaa ETH:ta synnytetttiin “ennakkolouhinnan”¹³ tuloksena, joka jaettiin Ethereum Foundationin ja noin 100 varhaisen Ethereum-protokollan kehittäjän kesken.¹⁴

Buterin on myöhemmin vaikuttanut katuvaan sitä, miten Ethereum-protokollan alussa ETH-varojen jakelu toteutettiin, mutta toisaalta huomauttaa, että hankkeen alkuaikoina ei välttämättä ollut vaihtoehtoja toteuttaa prosessia neutraalilla ja läpinäkyvällä tavalla.¹⁵

Ethereumin perustajatiimi onnistui kokoamaan ennätysellisen suuren – tuolloin noin 18 M\$ suuruisen – joukkorahoituksen julkisen Ethereum-lohkoketjuhankkeen ensimmäisen vaiheen toteuttamiseksi.¹⁶

Toukokuussa 2015 julkaistiin Ethereum *Olympic*-testiverkko ja heinä-elokuussa Ethereum-verkon ensimmäinen, *Frontier*iksi nimetty, versio. Ethereumin alkulohko louhittiin 30. heinäkuuta 2015 kello 01:26:13 Suomen aikaa.¹⁷

¹⁰ Matthew Leising 2021: *Out of the Ether: The Amazing Story of Ethereum and the \$55 Million Heist that Almost Destroyed it All*. Hoboken, NJ: Wiley.

¹¹ Armand Tanzarian 2014: [Ethereum Raises 3,700 BTC in First 12 Hours of Ether Presale](#). Cointelegraph.

¹² ETH:n tarjontadynamiikka on BTC:tä monimutkaisempi, jonka vuoksi “ennakkolouhitun” ETH:n määrä muuttuu ajan kuluessa. Lisätietoja Ethereumin liikkeeseenlaskusta, ks. slacknation: [Overview: Ethereum's initial public sale](#). Medium; Messari.io 2022: [Ethereum / Launch & Initial Token Distribution](#); Camila Russo 2021 [2020]: [Sale of the Century: The Inside Story of Ethereum's 2014 Premine](#). CoinDesk; Hasu 2020. [Twitter](#).

¹³ Tunnetaan englanniksi nimellä *premine*.

¹⁴ Vitalik Buterin 2022: [The roads not taken](#).

¹⁵ Ks. alaviite 14.

¹⁶ Daniel Palmer & Alyssa Hertig 2021 [2022]: [Who Created Ethereum?](#). CoinDesk.

¹⁷ Etherscan: [Block o](#)

Loppu on historiaa, josta on vielä monta lukua kirjoittamatta.¹⁸

Lue lisää Ethereumin historiasta



Ethereumin esiversio oli vajaan parikymppisen Vitalikin projekti...

Ultimate Scripting: A Platform for Generalized Financial Contracts on Mastercoin

0.1. Introduction

Perhaps the key advantage of Mastercoin over the open Bitcoin protocol is the potential to include much more advanced transaction types, including transactions that specify behavior based on future information well off into the future. For example, Mastercoin joins Ripple in being one of the only two major cryptocurrency networks that include the ability for users to make binding exchange offers as a type of transaction. Even then, the Mastercoin Foundation intends to integrate even more complex contracts, including bets, contracts for difference and on-blockchain derivatives. However, up until the point Mastercoin has been using a relatively unstructured process in developing these offers, essentially treating each one as a unique "hack" with its own consensus code and rules. This document outlines an alternative way of specifying Mastercoin contracts which follows an open-ended philosophy, specifying only the basic data and arithmetic building blocks and allowing anyone to craft arbitrarily complex Mastercoin contracts to suit their own needs, including needs which we may not even anticipate.

0.2. Specification

The underlying idea behind this specification is to allow anyone to create a contract which pays out according to an arbitrary formula. The formula will be defined in a Bitcoin-like stack-based scripting language, consisting of numbers and operators.

The evaluation algorithm is as follows:

```
stacktrack = []
opstack = []
while (len(stack) > 0):
    op = pop(stack)
    if op == 'push':
        val = stacktrack.pop()
        stacktrack.append(val)
    else:
        return stacktrack.pop()
```

Where eval is defined for each opcode below. Any error (eg. division by zero) will result in the entire transaction being treated as invalid by the Mastercoin network. All variables will be signed 64-bit integers, and all arithmetic operations wrap around (that is, if the underlying arithmetic operation returns A, the value pushed is (A + 2⁶⁴) % 2⁶⁴).

Ethereum: The Ultimate Smart Contract and Autonomous Corporation Platform on the Blockchain

In the last few months, there has been a great amount of interest into the area of using the Bitcoin blockchain, the mechanism that allows for the entire world to agree on the state of a public ownership database, for more than just money. Perhaps the first, and oldest, such alternative application is colored coins, which is a protocol that allows users to label specific Bitcoins and treat them as assets representing some real world value - whether company shares, collectibles or even existing currencies. But gold and USD, is more independent alternative. Rightly, also includes the ability to create custom currencies and assets, but adds a decentralized exchange. More recently, Mastercoin has started to go even further, allowing more complex financial contracts such as hedging, insurance derivatives, binary options and self-liquidating currencies - essentially, almost any common financial instrument imaginable. Taken together, all of these projects can be thought of as initial efforts toward a sort of "cryptocurrency 2.0" - they are to Bitcoin what Web 2.0 was to the World Wide Web circa 1995.

At the same time, there has been significant interest in "decentralized autonomous organizations" - autonomous entities that operate on the blockchain in a completely transparent and publicly managed way without any central control whatsoever. Rather than the relationships of the investors, owners and employees of the corporation being mediated by a legal contract or a set of organizational bylaws, the funds and corporate resources are managed directly on the blockchain. However, decentralized autonomous organizations are difficult to implement today, simply because the scripting systems of Bitcoin, and even post-cryptocurrency 2.0 alternatives like Ripple and Mastercoin, are far too limited to allow the kind of arbitrarily complex computation that DAOs require. Although these platforms have begun to offer increasingly complex contracts such as financial derivatives, order matching and more like that, the way that the protocols are set up is inherently limited and closed-ended: each of these cases is treated as a specific transaction type, not allowing any way for users to build contracts that the developers have not specifically chosen to include.

What this project intends to do is take cryptocurrency 2.0, and generalize it - create a fully-fledged, Turing-complete (but heavily (re-regulated) cryptographic) ledger that allows participants to encode arbitrarily complex contracts, autonomous agents and relationships that will be mediated entirely by the blockchain. On-chain currencies, future contracts, prediction markets, Namecoin-style domain name systems, and even possibly, fair gambling, sites will become trivial to implement, existing as simple, hardcoded lines of code on-chain on the chain.

Basic Building Blocks

Buterin työskenteli Mastercoinin tiimin kanssa lokakuussa 2013 protokollan parantamiseksi...

mutta päätyi uuteen lähestymistapaan myöhemmin marras-joulukuussa a 2013.

¹⁸ Ethereumin historiasta ja eri vaiheista on kirjoitettu kolme laajaa teosta: (1) Camila Russo 2020: The Infinite Machine: How an Army of Crypto-hackers Is Building the Next Internet with Ethereum. New York, NY: Harper Business, (2) Matthew Leising 2021: Out of the Ether: The Amazing Story of Ethereum and the \$5 Million Heist that Almost Destroyed it All. Hoboken, NJ: Wiley ja (3) Laura Shin 2022: The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze. New York, NY: PublicAffairs. BTC:n ja ETH:n markkinadominanssista, ks. kuvio 1 ja kuvio 2.

KUVIO 1. BITCOIN: MARKKINADOMINANSSI VUOSINA 2021–2022¹⁹



Lähde: TradingView

KUVIO 2. ETHEREUM: MARKKINADOMINANSSI VUOSINA 2021–2022



Lähde: TradingView

¹⁹ Markkinadominanssi johdonmukainen mittari yli ajan, koska m/n -tyylisessä laskelmassa bitcoinin ja kryptovaluuttojen kokonaismarkkina-arvo on eri aikoina jakautunut eri määrälle nimittäjässä olevia varallisuuseriä.

Työntodisteesta irtautuminen²⁰

"Ominaisuus, jonka ansiosta bitcoin on peukaloimatonta, ei ole 'lohkoketju', vaan työntodiste."

– **Andreas M. Antonopoulos**²¹

Buterin kirjoitti Ethereumin esitelleessä teknisessä kuvauksessa pitävänsä "todennäköisenä, että Ethereum siirtyy varantotodistemalliin".²²

Keskustelua PoW- ja PoS-konsensusmekanismeista käytiin Ethereumin perustajatiimin, kehittäjien, sijoittajien ja muiden aiheesta kiinnostuneiden välillä jo ennen Ethereumin julkaisua heinäkuun lopussa 2015.²³

Monet – mukaan lukien Buterin – olivat jo ennen tätä kiinnostuneita hahmottelemaan, miten ja milloin Ethereumin kaltainen julkinen lohkoketjujärjestelmä voisi siirtyä PoW-konsensusmekanismia paremmin skaalattavaan, turvallisempaan ja ympäristöystävällisempään²⁴ tapaan vahvistaa liiketoimet ja kirjata ne julkiseen lohkoketjuun.²⁵

Buterin oli innostunut vaihtoehtoista konsensusmekanismeista jo vuonna 2013 – ja on kutsunut työntodistetta myöhemmin "tuhlaamiseksi".²⁶ Kyse oli työntodisteelle vaihtoehtoisesta konsensusalgoritmista lohkoketjuprotokollan tasolla.²⁷

Protokollasäännöissä on kuitenkin kyse jostain aivan muusta kuin yksiulotteisista teknisistä valinnoista, koodin kauneudesta tai protokollan aiheuttamasta "hukasta".

²⁰ **PoS, Proof of Stake.** Tälle ei ole vakiintunutta suomennosta. Suomenkielisessä kirjallisuudessa on käytetty muun muassa "varantotodistetta", "sitomistodistetta", "osuustodistetta", "panostodistetta", "vakuustodistetta" ja "panttaustodistetta".

Staking, stake. Myöskään *steikkaukselle* ei ole vakiintunutta suomennosta. Suomenkielisessä kirjallisuudessa on käytetty muun muassa "varaamista/varantoa", "sitomista/sidos", "osuuttamista/osuus", "panostusta/panos" ja "panttaus/pantti".

²¹ Andreas M. Antonopoulos: The Internet of Money Volume Two. Merkle Bloom.

²² Vitalik Buterin 2022 [2014]: [A Next-Generation Smart Contract and Decentralized Application Platform](#).

PoS-konsensusmekanismin esittelivät Sunny King & Scott Nadal 2012: [PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake](#). White paper.

²³ juansgalt 2015: [So, Ethereum will Start with PoW, what PoS will it use and when will it switch?](#). reddit; Ethereum Homestead 2016: [History of Ethereum](#).

²⁴ Taylor Gerring 2016: [Cut and try: building a dream](#). Ethereum Foundation Blog.

²⁵ Esim. Vitalik Buterin 2014: [Slasher: A Punitive Proof-of-Stake Algorithm](#). Ethereum Foundation Blog. Se, että onko PoS-konsensusmekanismi PoW-konsensusmekanismia parempi näiltä osin, ei ole tämän kirjoituksen aiheena.

²⁶ Vitalik Buterin 2022: [Twitter](#).

²⁷ Erilaisista konsensusmekanismeista ja strategioista, ks. Wenbo Wang ym. 2019: [A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks](#). IEEE Access; H. S. Jennath & S. Asharaf 2020: [Survey on Blockchain Consensus Strategies](#). ICDSMLA 2019; Bahareh Lashkari & Petr Musilek 2021: [A Comprehensive Review of Blockchain Consensus Mechanisms](#). IEEE Access; Sonali Vyas ym. 2022: Blockchain Technology: Exploring Opportunities, Challenges, and Applications. Boca Raton, FL: CRC Press.

PoS-lohkoketjuihin liittyy perustavanlaatuisia ongelmia: miten on mahdollista samaan aikaan maksimoida “siirtojen nopeus, käyttäjäystävällisyys ja energiatehokkuus turvallisuudesta tinkimättä”.²⁸

Kyse on arvoista, kannustimista, hallinnosta, instituutioista ja valinnoista tilanteessa, jossa kukaan ei voi lähtökohtaisesti luottaa kehenkään muuhun – tai varsinkaan muiden oletettuun hyvántahtoisuuteen.²⁹ Tämä lähtökohta – *don’t trust, verify* – on peräisin kyberpunkkarikulttuurista, mutta se tuli todistetuksi myös Cynthia Dworkin ja Moni Naorin vuonna 1992 ilmestyneestä urauurtavasta tutkimuksesta pyrkii vähentää roskapostia eli eräänlaista palvelunestohyökkäystä.³⁰ Dworkin ja Naorin esittämä ajatus roskapostin torjunnasta perustui ajatukseen, jonka mukaan käyttäjän on suoritettava riittävä määrä laskennallista työtä (työntodiste) saadakseen oikeuden siirtää arvoa verkossa (esim. sähköpostin muodossa).

Työntodisteen nerokkuus on laskennallisten kulujen epäsymmetriassa: työntodistamisen pitää olla riittävän *vaikeaa* työntekijälle, mutta mahdollisimman *yksiselitteisesti* ja *helposti* todennettavissa kenelle tahansa ulkopuoliselle. Kymmenen vuotta myöhemmin brittiläinen kryptografi Adam Back otti kopin tästä ideasta ja kehitti *hashcashin* idean.³¹ Myöhemmin, kun Satoshi Nakamoto yhdisti vuonna 2008 ilmestyneessä bitcoinin toimintaa kuvanneessa teknisessä kuvauksessa työntodisteeseen digitaaliset allekirjoitukset, vaikeudensäätöalgoritmin ja hajautetun tilikirjan (lohkoketju), syntyi täysin ennennäkemätön digitaalinen eliölaji, *bitcoin*.³²

Buterin jatkoi varantotodistetta koskevia pohdintojaan ja julkaisi sitä koskevat ajatuksensa 31. joulukuuta 2016 ilmestyneessä kirjoituksessaan.³³

Ethereumin piirissä on aina ollut merkittävä PoS-konsensusmekanismin kannattajakunta: Buterin oli esittänyt sen *todennäköisenä* kehityssuuntana ja

²⁸ Chris Duckett 2022: [Ethereum sidechain Ronin that powers play-to-earn game is fleeced for over \\$600m](#). ZDNet.

²⁹ Ks. esim. Roberto Infante 2019: Building Ethereum Dapps: Decentralized Applications on the Ethereum Blockchain. Shelter Island, NY: Manning; Ioanid Rosu & Fahad Saleh 2021: [Evolution of Shares in a Proof-of-Stake Cryptocurrency](#). Management Science 67: 661–672.

³⁰ Cynthia Dwork & Moni Naor 1992: Pricing via Processing or Combatting Junk Mail. CRYPTO 1992: Advances in Cryptology — CRYPTO’ 92 pp 139–147

³¹ Adam Back 2002: [Hashcash – Amortizable Publicly Auditable Cost-Functions](#).

³² Satoshi Nakamoto 2008: [Bitcoin: Sähköinen käteisjärjestelmä vertaisverkossa](#).

³³ Vitalik Buterin [2016]: [A Proof of Stake Design Philosophy](#). Erilaiset PoS-konsensusmallit ovat saaneet osakseen runsaasti kritiikkiä, ks. Houy (2014), Bitfury Group (2015), Poelstra (2015), Sztorc (2015), Demeester (2017a, 2017b, 2019), Kelley (2017), Nguyen (2018a, 2018b, 2018c, 2019), McIntyre (2019), Deirmentzoglou ym. (2019), Voskuil (2019), factchecker (2020), Rettig (2021), Schwarz-Schilling ym. (2021), Schnitzer (2021), yanmaani (2021), Sus (2022).

Ethereumin kehittäjäyhteisö muotoili jo varhaisessa vaiheessa suunnitelmia PoS:iin siirtymiseksi.³⁴

Alun alkaen Ethereumiin suunniteltiin ehdoton haarauma (“vaikeuspommi”) jo lohkokorkeudessa 200 000 (syyskuu 2015)³⁵, jonka myötä saisi alkunsa “jääkaudeksi” kutsuttu eksponentiaalisesti vaikeutuvan louhinnan vaihe varantotodisteeseen siirtymiseen kannustamiseksi.

Vuosien varrella tämä toteutusmalli kohtasi monenlaisia haasteita, jonka vuoksi sen käynnistämisen ajankohtaa on siirretty toistuvasti tulevaisuuteen.³⁶



³⁴ [The Ethereum Merge](#) (2022); Ethereum Wiki: [Proof-of-Stake FAQs](#); Ethereum.org 2022: [Proof-of-stake \(PoS\)](#)

³⁵ Prabath Siriwardena 2017: [The Mystery Behind Block Time](#).

³⁶ Oliver Barsby 2022: [Ethereum Difficulty Bomb Date: EIP-4345 Seeks To Delay Difficulty Bomb Until June](#). Planet Crypto.

Ethereumin neljä kehitysvaihetta

“ETH 2.0 on viimeistelty turvallisuustarkastuksia lukuun ottamatta.”

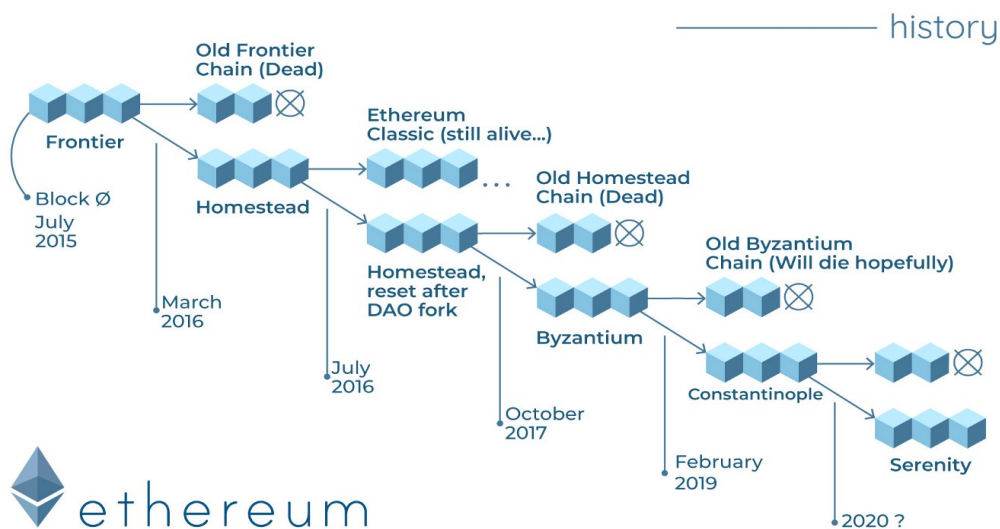
– Vitalik Buterin³⁷

Ethereum Foundation julkaisi noin viisi kuukautta ennen Ethereum-verkon käynnistymistä (eli ensimmäisen lohkon louhimista) vuonna 2015 neljästä erillisestä kehitysvaiheesta eli julkaisupaketeista koostuvan tiekartan.³⁸:

1. Frontier
2. Homestead
3. Metropolis
4. Serenity³⁹

Tiekartan neljä kehitysvaihetta (kuvio 3) kuvastavat Ethereumin kehityspolkua, jonka ytimessä on visio paremmin skaalattavasta, turvallisemmasta ja ympäristöystävällisemmästä julkisesta lohkoketjuverkosta.⁴⁰

KUVIO 3. ETHEREUMIN KEHITYSVAIHEET VUOSINA 2015–2019



Lähde: [Sara Ray](#) (2019) – Katso myös [ConsenSys](#) (2019)

³⁷ ConsenSys 2019: [30 Quotes that Defined a Momentous Ethereum Summit](#).

³⁸ Vinay Gupta 2015: [The Ethereum Launch Process](#). Ethereum Foundation Blog; Andreas M. Antonopoulos & Gavin Wood 2019: *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA: O'Reilly Media.

³⁹ [notes.ethereum.org](#) 2022: [Serenity Design Rationale](#)

⁴⁰ Julkinen lohkoketju on tietokanta ja tilikirja avoimessa (vihamielisessä) ympäristössä, jonka vuoksi ne kaikki kohtaavat niin sanotun lohkoketjutrilemman, ks. Timo Oinonen 2022: [Hajautettu rahoitus: Ethereum ja kilpailevat protokollat](#). Coinmotion Blog.

Tiekartta kuvaa myös Ethereumin vaiheittaista siirtymää pois työntodistekonsensuksesta ja hitaahkosta liiketoimien käsittelystä kohti varantodistepohjaista julkista lohkoketjua, jossa liiketoimien kirjaaminen lohkoketjuun on nopeaa ja siirtokulut pienemmät nykyiseen PoW-ketjuun verrattuna (ks. taulukko 1).

Buterinin vuonna 2015 esittämät arviot Ethereumin kehityskaaresta ovat osoittautuneet ylioptimistisiksi. Hän oli jopa omien sanojensa mukaan aliarvioinut ohjelmistokehityksen monimutkaisuuden (ks. kuva 1)⁴¹, jonka lisäksi korkeiksi paisuneet kulut PoW-konsensusalgoritmiin perustuvassa Ethereumissa ovat Buterinin mukaan rajoittaneet merkittävästi tavoin Ethereumin käytön yleistymistä muissa kuin rahoituspalvelusovelluksissa.⁴²

Samaan aikaan eräs Ethereumin tunnetuimmista pääkehittäjistä Péter Szilágyi ilmaisi maaliskuun puolivälissä huolensa Ethereum-protokollan monimutkaisuuden jatkuvasta kasvusta Twitter-ketjussa. Szilágyi on ollut mukana Ethereumin kehittämisessä jo vuosien ajan, joten hänen ajatuksensa saattavat hyvinkin kuvastaa laajemminkin Ethereumin kehittämisen parissa työskentelevien ajatuksia:

“Monimutkaisuus on järjestelmän usein ylenkatsottu näkökohta, koska yleensä joku maksaa siitä hintaa – ei sen aiheuttaja.

Älä uskottele muuta, sillä joku **maksaa** hinnan siitä rahan, ajan tai henkisten kykyjen muodossa. He eivät ehkä halua/voi tehdä niin ikuisesti.

Skaalautuvuuden tavoin myös monimutkaisuus kasautuu huomaamatta aina murtumispisteeseen asti. Silloin [monimutkaisuus] on jo ohittanut jo kynnyksen, jonka jälkeen ei ole enää paluuta.

Monimutkaisuudella on myös se ikävä vaikutus, että se aiheuttaa kasautuvia ongelmia. – –

Ethereumin historiassa monimutkaisuus ei ole koskaan vähentynyt, vaan jokainen Ethereumin parannusehdotus on kasautunut [edellisten] päälle. Jokainen suuri muutos – – on yksi napsu lisää [monimutkaisuutta].

Olen äärimmäisen turhautunut, kun tutkimusehdotuksessa sanotaan, että “kaikki on jo selvitetty, nyt on vain kehitettävä.”

⁴¹ Vitalik Buterin 2022: [Twitter](#).

⁴² Andrew R. Chow 2022: [I Spent 80 Minutes Inside Vitalik Buterin's Brain. Here's What I Learned](#). TIME.

Minun on korostettava – niin hyvältä kuin The Mergen lähestyminen tuntuukin – ettei Ethereum ole matkalla selkeään suuntaan. [Ethereum] saavuttaa etäisesti tuloksia, mutta se myös kasaa monimutkaisuutta ikään kuin huomista ei olisi.

Jos protokolla ei laihdu, se ei selviä.

Mielestäni perimmäinen syy on tutkimuksen ja kehitystiimien välinen epäsuhta. Ensin mainitun on “vain” keksittävä tyylikkäitä – yksittäisiä – ideoita.

Jälkimmäisen tehtävänä on jonglöörata kaikkien koskaan esitettyjen ideoiden kanssa ja samalla kirurgisesti laajennettava avaruuden ulottuvuuksia.

Monimutkaisuutta on yritetty vähentää – –. Protokollan monimutkaisuutta ei kuitenkaan ole koskaan yritetty vähentää.

Olemme jo ohittaneet sen pisteen, jossa kenelläkään olisi täydellinen kuva järjestelmästä. Tämä on ikävä asia.

En osaa sanoa, miten tämä pitäisi ratkaista, mutta vaatimaton mielipiteeni on, että lopetetaan ominaisuuksien lisääminen ja ryhdytään karsimaan, vaikka siinä samalla rikottaisiin jotain.

Yhä harvemmat ihmiset osaavat ja haluavat parsia kokoon rikkinäistä verkkoa. Ja jokainen muutos etäännyttää entistä enemmän.”⁴³

Monta vuotta jatkuneet tutkimus- ja kehityssponnistelut ovat olleet mutkikkaita⁴⁴, mutta niiden aikana on vahvistunut halu siirtyä varantotodisteeseen. Vuodesta 2016 alkaen on toteutettu neljä keskeistä ehdotonta haaraumaa PoS-vision edistämiseksi.⁴⁵

PoS-lohkoketjussa liiketoimien vahvistamisesta vastaavat validaattorit eli vahvistajasolmut, jotka *varaavat*⁴⁶ Ethereumin tapauksessa ETH:ta osallistuakseen PoS-liiketoimien vahvistamiseen. Mitä enemmän validaattori sitoo ETH:ta verkon hyväksi, sitä todennäköisemmin se voittaa lohkonvahvistusarpajaiset ja saa voittaessaan vaivanpalkaksi vahvistusarpajaisten lohkopalkkion.⁴⁷

⁴³ Péter Szilágyi 2022: [Twitter](#).

⁴⁴ SFOX 2018: [From Crowdfunded Blockchain to ICO Machine: An Ethereum Price History](#). Yhteenveto Ethereumin päivityksistä ja ehdottomista haaraumista, ks. ConsenSys 2019: [A Short History of Ethereum](#); Luit Hollander 2020: [History of Ethereum Hard Forks](#).

⁴⁵ ethereum.org 2022: [The history of Ethereum](#). Ks. myös Okereke Innocent 2021: [History Of Ethereum Hard Forks](#).

⁴⁶ Ks. alaviite 12.

⁴⁷ Varantotodiste on konsensusprotokolla, jossa liiketoimien vahvistaja, lohkon tuottaja ja lohkon lisääjä (bitcoinissa tämä vastaa louhijaa, mutta PoW ja PoS ovat aivan erilaisia konsensusmalleja) valitaan määritellyn suuruisen todistettavan ja taloudellisesti mielekkään varanto-osuuden (ts. kolikoiden määrä, jotka tietty vahvistaja on sitonut

TAULUKKO 1. TYÖNTODISTEEN JA VARANTOTODISTEEN YLEISTÄ VERTAILUA

	Työntodiste (PoW)	Varantotodiste (PoS)
Energiankulutus	Korkea, koska PoW-louhinta	Matala, koska PoS-validointi
Työkalut & tuotantoprosessi	Erityiset louhintalaitteet (GPU ja ASICS); louhinta "ulkoista"	Validaattorisolmu (tehokas pöytätietokone); validointi "sisäistä"
Väärentämätön kalleus⁴⁸	Kyllä	Ei
Turvallisuus/Lopullisuus	Mitä enemmän laskentatehoa on verkon suojana, sitä turvallisempi verkko; probabilistinen malli & todennettu	Steikkaus turvaa verkon toiminnan ja uusien lohkojen tuotannon; edelleen suhteellisen uusi julkisissa ketjuissa
Skaalautuvuus	L1:ssä suhteellisen matala, L2:ssa korkea; L2:n tarjoaa lukuisia mahdollisuuksia, jonka lisäksi ketjussa olevia bitcoineja voidaan lukita ja hyödyntää toisen (lohkoketju)verkon ja/tai keskitetyn tahon toimesta; myös yksityisiä avaimia voidaan siirtää toimijalta toiselle verkon ulkopuolella (vrt. Opendime)	Laskennallisesti korkea jo L1-tasolla ja L2 kasvattaa entisestään (turvallisuus on trade-off); monikerroksinen skaalaaminen ⁴⁹
Keskittymisaste	Verkossa hajautuneisuus toteutuu usealla asteella, louhinnan keskittyneisyys on merkittävin uhka; muutoin hajautettu monella tasolla	PoS-algoritmi valitsee validoinnin voittajan: mitä enemmän steikattuna, sitä suurempi todennäköisyys voittaa; keskittyminen mahdollista
Haaraumat	Objektiiviset: kannustimet ohjaavat hakeutumaan suurimman työn omaavaan työntodistetekstuun	Subjektiiviset: ei automaattisia kannustimia ehkäisemään haaraumia

Lähde: BitFury Group (2015), McIntyre (2019), Blockworks (2022), Lashkari & Musilek (2021), Cointelegraph (2022)

verkon liiketoimien vahvistamiseen). PoS-konsensusalgoritmin tärkeimpinä etuina pidetään sen väitetysti parempaa turvallisuutta ja energiatehokkuutta.

⁴⁸ PlanB 2019: [Twitter](#).

⁴⁹ Alex Gluchowski: [Evaluating Ethereum L2 Scaling Solutions: A Comparison Framework](#)

KUVA 1. BUTERININ ALKUPERÄISET ARVIOT OSOITTAUTUIVAT YLIOPTIMISTISIKSI



vitalik.eth ✓
@VitalikButerin

...

3. My projections from 2015 of when we will get PoS and sharding. Honestly, these were very wrong and worth laughing at; I'll share a screenshot of one of my presentations from 2015 so everyone can laugh more easily.

Käännä twiitti

Launch roadmap

- Frontier (6 days ago!)
- Homestead (2-4 months)
- Metropolis (4-8 months, Mist)
- Serenity (6-12 months, PoS)
- Virtual machine upgrades (1.2?)
- Scalability (2.0?)

12.14 ap. · 2. tammik. 2022 · Twitter Web App

Lähde: Vitalik Buterin (2022)

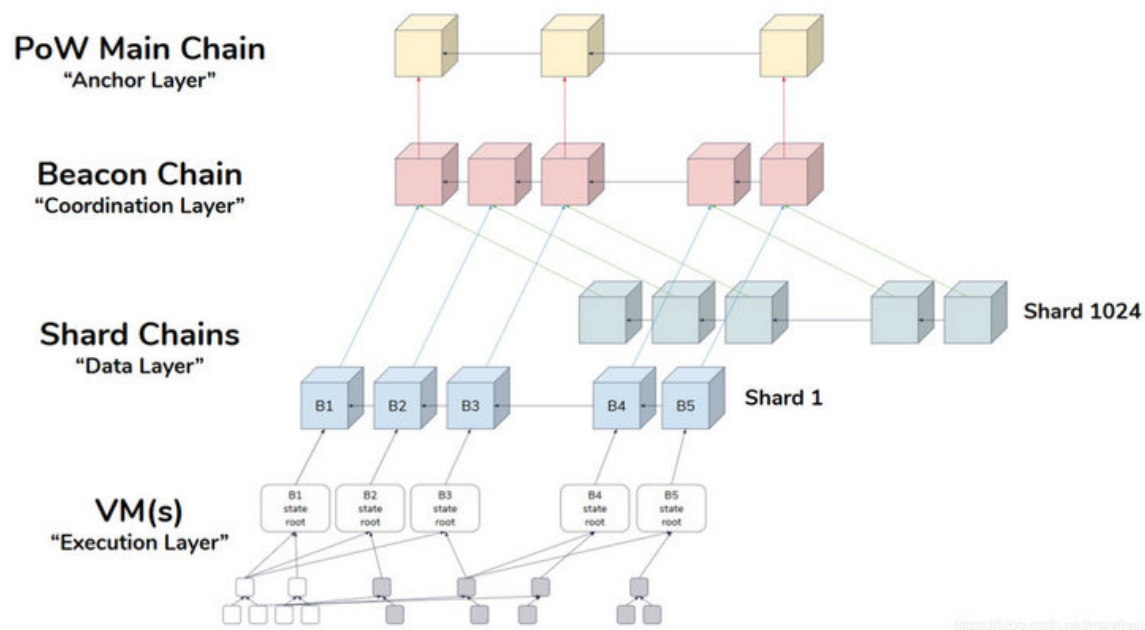
Tyyneys kulman takan? – Lyhyt johdanto Serenity-vaiheeseen

“Tarvitaan maksimaalista desentralisaatiota luottamuksen infrastruktuurin rakentamiseksi.”

– Joe Lubin⁵⁰

Ethereum siirtyi vuonna 2020 viimeiseen kehitysvaiheeseen, jonka tuloksena odotetaan syntyväksi Ethereum 2.0 (ks. kuvio 4). Sen ytimessä on yksi uusi Beacon Chainiksi ristitty PoS-ketju ja lukuisia sirpaleiksi kutsuttuja Ethereum-lohkoketjun osasia.

KUVIO 4. “ETHEREUM 2.0” KORKEAN TASON ARKKITEHTUURI



Lähde: Developer Paper (2022)

Serenity-vaihe, jota joskus kutsutaan myös Ethereum 2.0:ksi⁵¹, koostuu kolmesta askeleesta:

1. Ensimmäisessä vaiheessa tapahtui PoS-konsensusmalliin perustuvan (alussa varsin) steriilin **Beacon Chainin** käyttöönotto 1. joulukuuta 2020 Ethereumin

⁵⁰ ConsenSys 2019: [30 Quotes that Defined a Momentous Ethereum Summit](#).

⁵¹ Tarkempi katsaus Ethereum 2.0:sta, ks. Mark Cole & CryptoEQ 2022: [Ethereum Upgrade Guide 2022](#). CORE+ Report

nykyisen pääketjun rinnalla⁵², kun marraskuussa 2020 julkaistun ETH2-talletussopimuksen⁵³ minimiit saatiin täytettyä viimeisenä päivänä.⁵⁴ Beacon Chain on Ethereum 2.0 -toteutuksen ytimessä ja se koordinoi ja varmistaa uuden verkon toiminnan.⁵⁵

Tällä hetkellä yli 336 000 validaattoria on pantannut⁵⁶ lähes 11 miljoonaa ETH:ta Beacon Chainin yksisuuntaiseen⁵⁷ älysovimukseen. Validaattorit vastaavat Beacon Chainin liiketoimien käsitlemisestä, datan tallentamisesta ja lohko-tuotannosta. Validaattorit ovat välttämätön edellytys sille, että Ethereum-verkon rinnakkaisketju kykenee tuottamaan uusia lohkoja – ja PoW-Ethereum voi siirtyä Beacon Chainin ohjauksessa PoS-konsensusmekanismiin.

2. Toisessa vaiheessa Ethereum-pääverkko ja Beacon Chain sulautuvat (*The Merge*; ks. Kuvio 5) muodostaen yhtenäisen verkon.⁵⁸ Näin Ethereumin konsensusprotokolla ja -parametrit muuttuvat ja käytännössä koko verkko siirtyy PoS-konsensusmekanismiin. Tämän myötä odotuksissa on verkon tehokkuuden, sensuroimattomuuden ja hajautuneisuuden parantaminen, mutta tässä vaiheessa verkon käyttökustannukset eivät vielä varsinaisesti laske. Sulautuminen on tällä hetkellä kuuma puheenaihe ja asia kiinnostaa monia (ks. kuvio 6).

⁵² Englanniksi nämä tunnetaan nimillä "Beacon Chain" (Eth2/ETH2, "konsensuskerros", PoS-konsensusmekanismi) ja "Ethereum mainnet" (Eth1, "toteutuskerros", PoW-konsensusmekanismi). Lue lisää Beacon Chainista: ethereum.org.

⁵³ Kyse ei ole sananmukaisesta talletuksesta, vaan

⁵⁴ Tämä "deposit contract" -niminen älysovimus elää nykyisessä Ethereum-verkossa ja siihen siirrettyjä ETH-varoja ei voi enää käyttää PoW-Ethereum-verkossa, koska ne on *steikattu*. Minimivaade on 32 ETH. Ks. myös William Foxley 2021 [2021]: [Ethereum 2.0 Beacon Chain Goes Live as 'World Computer' Begins Long-Awaited Overhaul](#). CoinDesk; Antti Hyppänen 2020: [Ethereum 2.0 opas](#). Bitcoinkeskus.com.

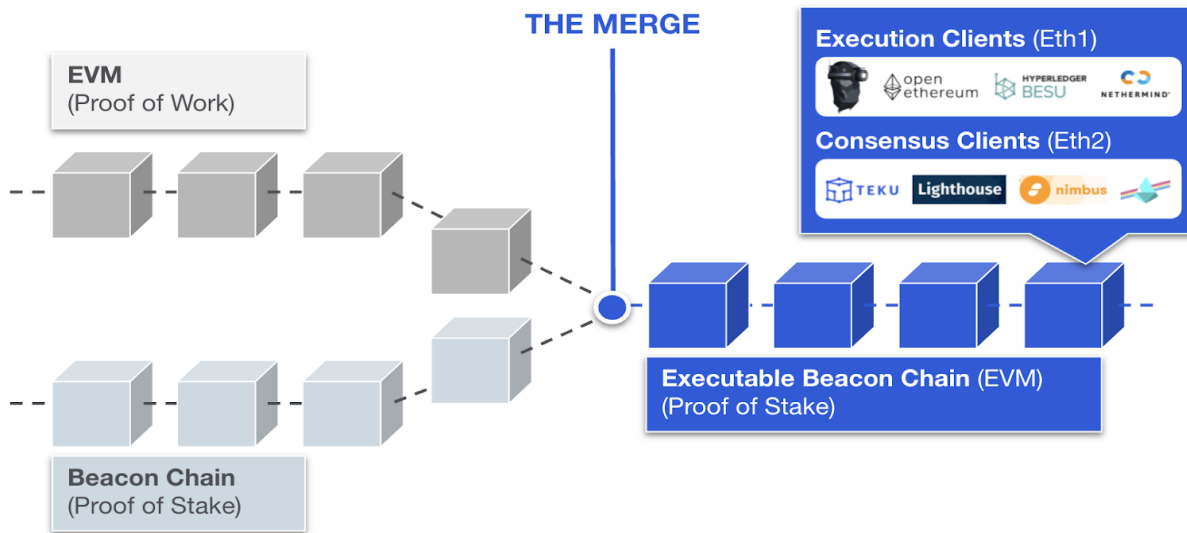
⁵⁵ James Beck 2020: [The Ethereum 2.0 Beacon Chain is here. Now what?](#). ConsenSys Blog.

⁵⁶ Nansen: [ETH2 Deposit Contract](#) (25.3.2022); ks. Yash Kamal Chaturvedi 2021: [All About The Validator In Ethereum 2.0 Beacon Chain](#). EtherWorld.co.

⁵⁷ ethereum.org 2022: [Ethereum staking](#); Cointelegraph: [Ethereum 2.0 staking: A beginner's guide on how to stake ETH](#).

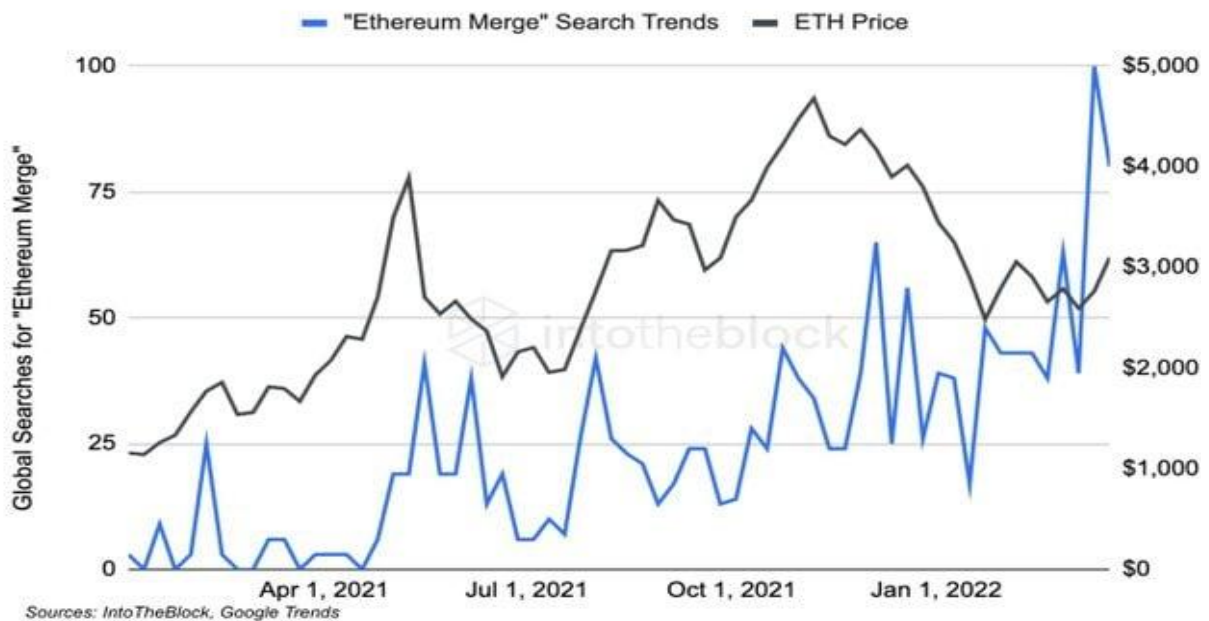
⁵⁸ [The Ethereum Merge](#) (2022).

KUVIO 5. SULAUTUMISEN JÄLKEISEN ETHEREUMIN KONSENSUS- JA TOTEUTUSKERROKSET



Lähde: ConsenSys (2021)

KUVIO 6. "ETHEREUM MERGE" -HAUT OVAT KASVANEET VUODESTA 2021



Lähde: IntoTheBlock

3. Kolmannessa vaiheessa Ethereum-verkko **sirpaloitetaan** (engl. *sharding*).⁵⁹ Tässä yhteydessä Ethereum-lohkoketju sirpaloituu lukuisiksi sirpaleiksi (engl. *shards*; “sirpaleketjut”) kutsutuiksi Ethereum-ketjun palasiksi, joten jokainen sirpale ei sisällä kaikkea tietokantaan tallennettua dataa.⁶⁰ Sirpaleet turvataan, niitä koordinoidaan ja ne synkronoidaan Beacon Chainin avulla. Sirpaloittamisen oletetaan kasvattavan Ethereum-verkon tehokkuutta ja kapasiteettia, jonka myötä myös liiketoimikulujen oletetaan laskevan merkittävästi. Tätä vaihetta kutsutaan nimellä *The Surge*.⁶¹

Buterin sirpaloittamisesta vuonna 2018

Kuvittele, että Ethereum on jakaantunut tuhansiksi saariksi. Kaikki saaret voivat tehdä omia juttujaan. Kaikilla saarilla on omat ainutlaatuiset ominaisuutensa, ja kaikki kyseiseen saareen kuuluvat, eli tilit, voivat olla vuorovaikutuksessa keskenään, ja ne voivat vapaasti hyödyntää kaikkia sen ominaisuuksia. Jos ne haluavat ottaa yhteyttä muihin saariin, niiden on käytettävä jonkinlaista protokollaa.



Buterin sirpaloittamisesta vuonna 2022

Ethereumin olosuhteet ja rajoitteet huomioon ottaen sirpaloittamisen yksinkertaistaminen ja korkeasta kunnianhimosta luopuminen oli mielestäni täysin oikea ratkaistu. Tästä huolimatta kunnianhimoisella tutkimuksella on myös erittäin tärkeä tehtävä: sen avulla tunnistetaan lupaavia tutkimussuuntia, sillä jopa hyvin monimutkaisista ideoista on usein “kohtuullisen yksinkertaisia versioita”, jotka ovat silti hyvin hyödyllisiä. Pidän hyvin mahdollisena mahdollista, että tämä vaikuttaa merkittävästi Ethereumin protokollakehitykseen (tai jopa toisen kerroksen protokoliin) tulevinä vuosina.”



⁵⁹ ethereum.org 2022: [Shard chains](#); Vitalik Buterin 2021: [Why sharding is great: demystifying the technical properties](#).

⁶⁰ Henri Heinonen 2018: [Kryptovaluutoista ja lohkoketjuista – osa 4](#). Luentomateriaalit.

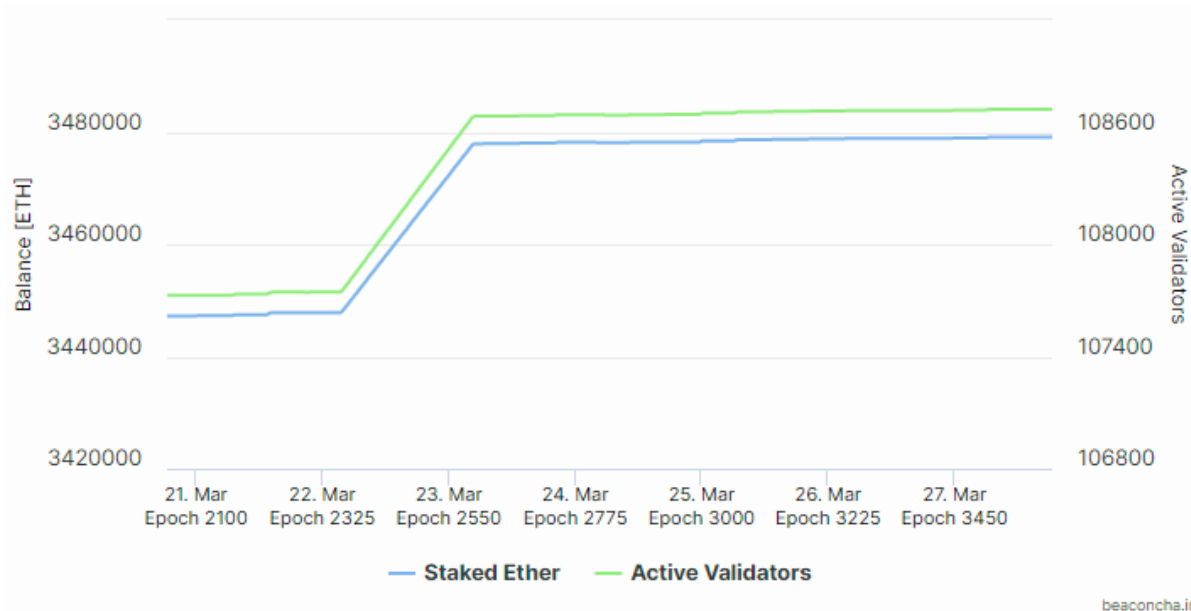
⁶¹ Vitalik Buterin 2022: [The roads not taken](#).

Kiln-testiverkko siirrettiin onnistuneesti varantotodisteeseen

15. maaliskuuta 2022 saatiin myönteinen signaali Ethereumin varantotodistepohjaiseen konsensusmalliin siirtymisestä.⁶² Ethereumin monivuotinen matka kohti PoS-konsensusmekanismia on nyt askeleen lähempänä, kun Ethereum-kehittäjät onnistuivat toteuttamaan **sulautumisen Ethereumin julkisessa Kiln-testiverkossa** eli siirtymään PoW-konsensusmallista PoS-malliin.⁶³ Uutinen otettiin innolla vastaan, koska Kiln-testiverkossa suoritettu sulautuminen oli osoitus siitä, että se on mahdollista teknisesti toteuttaa.

Kiln muistuttaa Ethereumin pääverkkoa ja se on alun alkaen toteutettu työntodistepohjaisena. Testisulautumisen ansiosta Kiln toimii nyt kuitenkin vakuudellisen mallin varassa. Kiln-tutkan mukaan noin 3,5 miljoonaa testi-ETH:ta on lukittu ja aktiivisia validaattoreita on noin 108 000 kappaletta (ks. kuvio 7).⁶⁴

KUVIO 7. ETHEREUMIN KEHITYSVAIHEET JA SULAUTUMISEN JÄLKEISET PÄIVITYKSET



Lähde: Kiln Explorer ([2022](#))

Ethereum Foundation on kehottanut Ethereumin ohjelmistokehittäjiä, solmujen ylläpitäjiä, vahvistajia (panttaajia) ja ekosysteemin muita toimijoita jatkamaan

⁶² Shaurya Malwa 2022: [Ethereum Merge Takes Place on Kiln Testnet](#). CoinDesk; Laszlo Dobos 2022: [Ethereum PoS testnet Kiln launched, merged and kickin'](#). CryptoSlate.

⁶³ Sulautumisen jälkeistä verkkoa mallintanut Kintsugi-testiverkko ei toiminut alkuvuodesta niin kuin toivottiin, ks. Laszlo Dobos 2022: [Ethereum merge testnet Kintsugi split by bug, here's why](#). CryptoSlate.

⁶⁴ beaconcha.in 2022: [Kiln Explorer](#).

testausta PoS-Kilnissä.⁶⁵ Seuraavassa vaiheessa myös kaikki muut Ethereumin julkiset testiverkot⁶⁶ ja konsensusohjelmistot⁶⁷ päivitetään PoS-yhteensopiviksi, jonka myötä koko Ethereum-verkon toivotaan siirtyvän PoS-konsensusmekanismiin vielä ennen tämän vuoden loppua.

Julkilausuttuna tavoitteena on toteuttaa siirtymä ennen loppuvuotta 2022 – ja nyt kertomus Ethereumin siirtymisestä kohti uutta kehitysvaihetta näyttää saavuttaneen myös perinteisen median (ks. kuva 2).⁶⁸

Ethereumin sulautumisen ja lohkoketjun sirpaloittamisen (*The Surge*) jälkeen seuraavat *The Verge*, *The Purge*- ja *The Splurge*-nimiset päivitykset (ks. kuvio 8). Pidemmällä tähtäimellä sulautuminen saattaa osoittautua kaikista *Serenity*-kehitysvaiheen askeleista yksinkertaisemmaksi, eikä sekään tule olemaan läpihuutojuttu.⁶⁹

Video: Ethereum-kehittäjät seurasivat Kiln-testiverkon sulautumista 15. Maaliskuuta 2022



⁶⁵ Protocol Support Team 2022: [Announcing the Kiln Merge Testnet](#). Ethereum Foundation Blog.

⁶⁶ Näillä viitataan mm. Görliin, Ropsteniin ja Kovaniin, ks. pseudotheos 2022: [Twitter](#).

⁶⁷ Näillä viitataan mm. Prysmiin, Lighthouseen ja Nimbusiin, ks. Pintail's Notes: [Comparing Eth2 Clients on the Medalla Network](#).

⁶⁸ Liam J. Kelly 2022: Ethereum 2.0 Coming in Q2, 'Will Lay to Rest' Energy Concerns: Joe Lubin. Decrypt.

⁶⁹ Ground Zero 2022: [GZ Daily — The Merge, Surge, Verge, Purge, and Splurge of the Ethereum Blockchain](#).

KUVA 2. CNBC VIITTAA TALOUSUUTISISSA SULAUTUMISEEN JA "ETHEREUM 2.0:AN"



Crypto-Gucci.eth 9m
@CryptoGucci

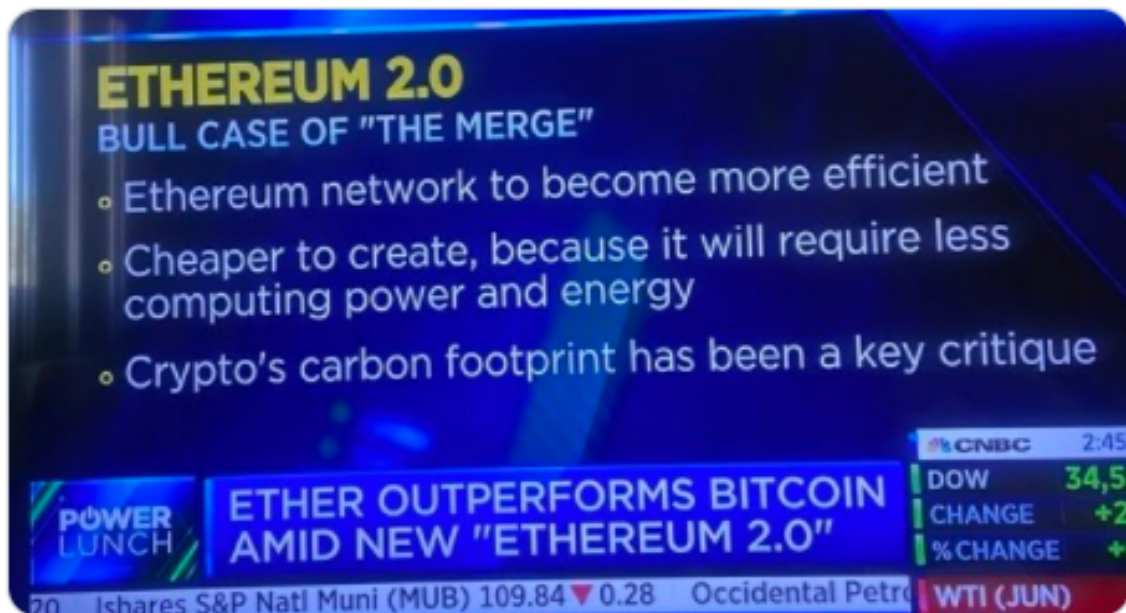
...

CNBC ran a segment today around [#Ethereum](#) outperforming [#Bitcoin](#)  amid new "Ethereum 2.0"

The narrative around the Ethereum Merge is finally getting out in the mainstream media

It won't be long before the world grasps the power of Ethereum

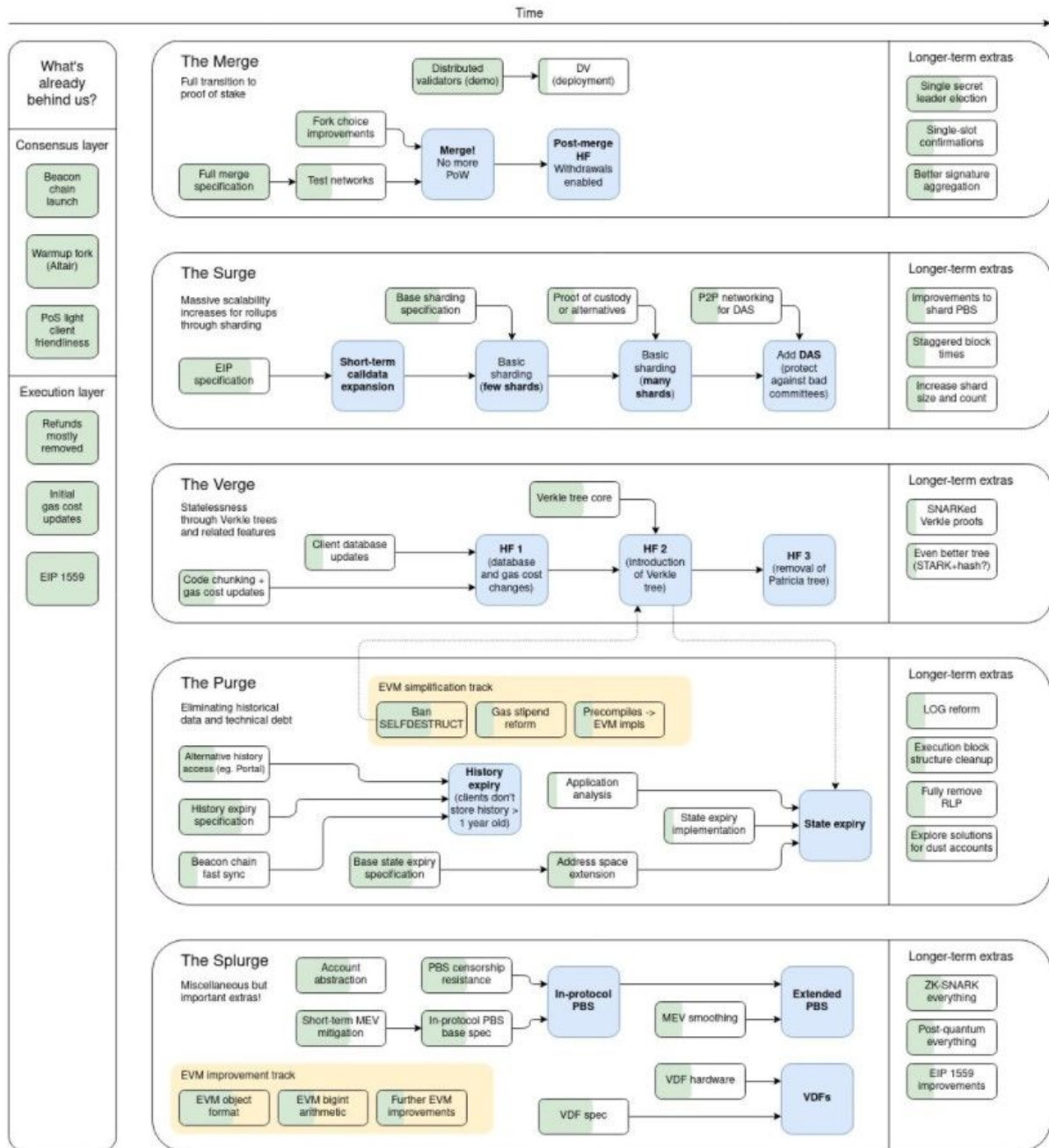
[Käännä twiitti](#)



11.35 ip. · 24. maalisk. 2022 · Twitter for Mac

Lähde: [Crypto-Fucci.eth](#) (2022)

KUVIO 8. ETHEREUMIN KEHITYSVAIHEET JA SULAUTUMISEN JÄLKEISET PÄIVITYKSET



Lähde: Vitalik Buterin (2021)

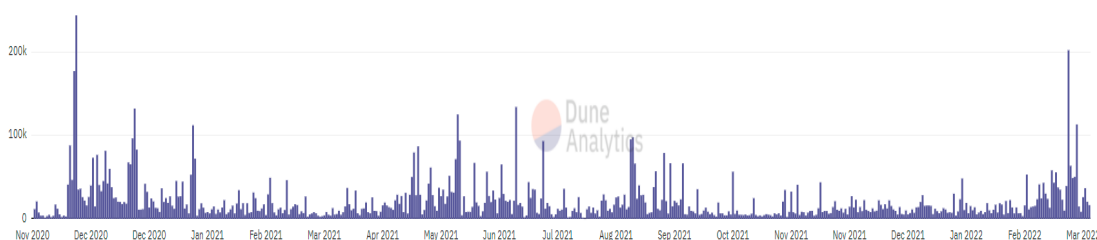
ETH2-panttaamisen suosio jatkaa kasvuaan

“PoS-konsensusmekanismin tavoitteena on olla tehokkain tapa pitää julkinen lohkoketju validoituna, ei maksimoida [liiketoimien] käsittelypalkkioita tietyissä tilanteissa.”

– Vitalik Buterin⁷⁰

Steikkaaminen on usein mielletty hieman harhaanjohtavasti “passiiviseksi tulonlähteeksi”, mutta tämä ei ole totta. Esimerkiksi tällä hetkellä ETH2-panttaus sitoo varat määräämättömäksi ajaksi ETH2-älysopimukseen, jonka vuoksi liiketoimien vahvistaja ei voi saada niitä takaisin ennen kuin toiminto on käytössä Beacon Chainissa.

KUVIO 9. PÄIVITTÄIN LUKITUT UUDET ETH-MÄÄRÄT BEACON CHAININ JULKAISEMISEN JÄLKEEN



Lähde: DuneAnalytics

Panttaamisen riskejä tarkastellaan tyypillisesti älysopimuksen turvallisuuden, protokollasääntöjen hallinnan (governance), validaattorin toiminnan, sääntelyn ja toisinaan steikkauspalveluita tarjoavien (epä)luotettavuuden aiheuttamien riskien näkökulmasta. PoS-lohkoketjussa validaattori voi myös menettää (ainakin osittain) vahvistamiseen lukitsemansa varat. PoS-konsensusmalleihin on esimerkiksi usein sisällytetty kannustimia, jotka ohjaavat validaattoreita olemaan mahdollisimman luotettavasti koko ajan vahvistamassa liiketoimia – ja jos jostain syystä validaattori ei ole verkossa protokollan määräämällä tavalla, siitä voi koitua rangaistus.⁷¹

Lisäksi on huomioitava, että valitettavan harvoin huomio kiinnittyy panttaamisen vaihtoehtoiskustannuksiin ja niiden aiheuttamiin riskeihin.⁷² Steikkaus voi aiheuttaa vaihtoehtoiskustannuksia ainakin kolmella tavalla, kun

⁷⁰ ConsenSys 2019: [30 Quotes that Defined a Momentous Ethereum Summit](#).

⁷¹ Ks. esim. Michael Neuder ym. 2021: [Low-cost attacks on Ethereum 2.0 by sub-1/3 stakeholders](#). arXiv:2102.02247.

⁷² Giulia Fanti ym. 2019: [Economics of Proof-of-Stake Payments Systems](#). Artikkeliluonnos.

1. käyttäjä ei tiedä milloin varat ja steikkaustuotot ovat taas käytettävissä;⁷³
2. käyttäjän steikkaustuottojen likviditeetti ja hinnanmuodostus saattavat olla heikkoja;
3. käyttäjän PoS-siirtymää varten sitoma ETH ei ole käytettävissä esimerkiksi vakuutena sinänsä tai hyödynnettävissä DeFi-sijoituksissa; ja
4. validaattorisolmun ajaminen ja ylläpitäminen vaativat omanlaistaan osaamista, joten opetteluun menee aikaa ja vaivaa.⁷⁴

Ethereumissa ETH2-lukitus edellyttää 32 ETH:n lukitsemista Beacon Chainin ETH2-älysopimukseen määräämättömäksi ajaksi. Jo pelkästään ETH-varat validointisolmun ajamiseksi maksaisivat ETH:n nykyhinnoilla melkein 100 000 euroa.

Monet kryptovaluuttapörssit, -vaihtopaikat ja muut toimijat ovat havainneet tässä markkinaraon tarjoten asiakkailleen mahdollisuuden lukita myös pienempiä määriä ETH:ta PoS-ETH2-talletussopimukseen.⁷⁵

Tällä hetkellä suurin ETH2-panttausta tarjoavista toimijoista on Lido, joka toimii desentralisoituna autonomisena organisaationa ja tarjoaa steikkaussyndikaattipalveluita⁷⁶ useille eri PoS-lohkoketjuille.⁷⁷

Lido on älysopimus, joka vastaa ETH-talletuksista ja -nostoista, stETH-tokenien tuottamisesta ja polttamisesta ja niin edelleen. Lidosta on tullut lyhyessä ajassa yksi suurimmista DeFi-projekteista, sillä siihen kokonaisuudessaan lukittu arvo on noin 16,7 miljardia dollaria ja sillä on ETH2-steikkauksessa hallitseva markkina-asema.⁷⁸

Mitä enemmän liiketoimien vahvistajat ovat sitoneet ETH:ta PoS-älysopimukseen, sitä matalampi on steikkauksen tuotto-odotus (ks. kuvio 10).

ETH-panttaajien ja pantattujen varojen määrä ovat jatkaneet kasvuaan tämän vuoden alkupuolelta alkaen (ks. kuvio 11). Alkuvuodesta alkaen ETH2-panttaussopimukseen on lukittu suuria määriä ETH:ta.⁷⁹ ETH2-sopimukseen lukittu ETH-määrä vastaa noin

⁷³ Lin William Cong ym. 2022: [Staking, Token Pricing, and Crypto Carry](#). SSRN.

⁷⁴ RBC office 2021: [Lido — the biggest beneficiary of Ethereum 2.0](#).

⁷⁵ Lu Yaoyuan 2021: [ETH2 Staking | Discovering the Value of Bloxstaking\(CDT\)](#).

⁷⁶ Englanniksi *staking pool*. Ks. esim. Mirko Schmiedl 2020: [How to stake ETH | The ultimate Ethereum 2.0 staking guide](#). Staking Rewards; Hans Gersbach ym. 2022: [Staking Pools on Blockchains](#). arXiv:2203.05838v1.

⁷⁷ Footprint Analytics 2022: [What made Lido a top ETH staking platform?](#). CryptoSlate.

⁷⁸ Anita Ramaswamy 2022: [How Lido raises the stakes for crypto and DeFi investors](#). TechCrunch.

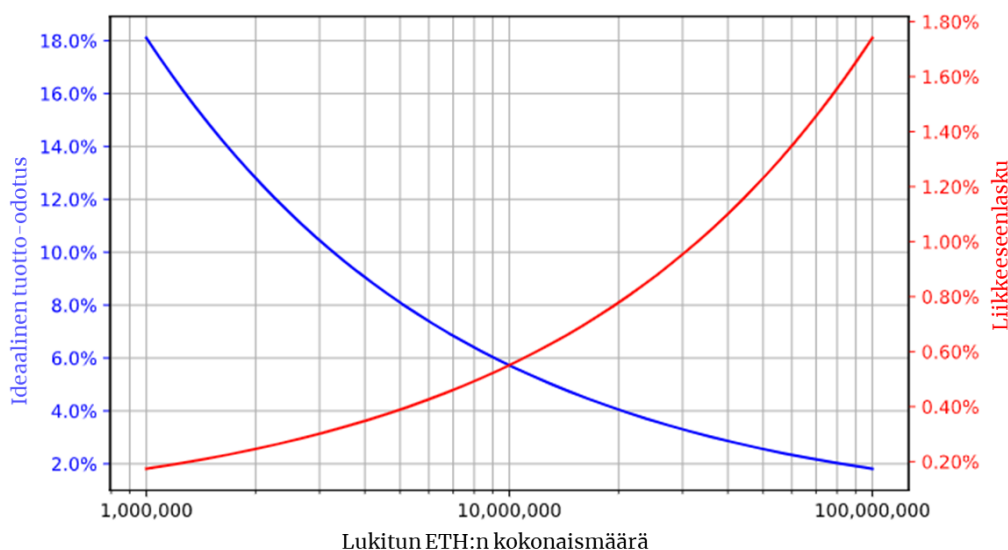
⁷⁹ Etherscan: [Contract 0x00000000219ab540356cBB839Cbe05303d7705Fa](#); Nansen: [ETH2 Deposit Contract](#) (25.3.2022)

9 %:ia ETH:n tämänhetkisestä tarjonnasta.⁸⁰ Samaan aikaan liikkeellä olevan ETH:n määrä vähenee viime vuoden elokuussa EIP-1559-päivityksen myötä käyttöönotettujen “polttomekanismien” ansiosta (ks. kuvio 12).⁸¹

Viime vuonna erilaisia pääasiassa steikkaukseen keskittyvä Staked lanseerasi Staked Eth Trust⁸², sveitsiläinen Sygnum Bank ryhtyi tarjoamaan institutionaalisia steikkauspalveluita⁸³ ja tämän vuoden maaliskuussa kävi ilmi, että Goldman Sachs saattaa olla suunnittelemassa Galaxy Digitalin Galaxy ETH Fund -sijoitustuotteen tarjoamista tietyille asiakasryhmälleen.⁸⁴

Osa kryptomarkkinoita seuraavista toimiala-analyytikoista on ennakoinut steikkauksen muuttuvan aikojen saatossa “Staking-as-a-Service” -tyyliseksi vaivattomaksi “tilauspalveluksi”, mutta todennäköisesti tässä saattaa mennä vielä vuosia ennen kuin tällaiset palvelut saavuttavat laajempaa suosiota.⁸⁵

KUVIO 10. LUKITUN ETH:N KOKONAISMÄÄRÄ VERRATTUNA VUOTUISEEN LIIKKEESEENLASKUUN (INFLAATIO) JA VALIDOINNIN TUOTTO-ODOTUKSEEN (PALKKIO)



Lähde: Onur (2019)

⁸⁰ Fredrik Vold 2022: [Ethereum Staking Sees Accelerating Growth Ahead of Merge](#). Cryptonews; Taylor Locke 2022: [Ethereum's blockchain is nearing a huge turning point that could push Ether's market value ahead of Bitcoin's](#). Fortune.

⁸¹ Liam J. Kelly 2022: [Nearly \\$6 Billion in ETH Burned as Ethereum 2.0 Edges Closer](#). Decrypt. Tarkempaa tietoa EIP-1559-päivityksestä (“London hard fork”) ja sen vaikutuksesta Ethereumin verkkodynamiikkaan, ks. Ali Abaday. 2021: [What is Ethereum London Hard Fork?](#). Coinmotion Blog. Poltettuja ETH-määriä voi seurata esimerkiksi: <https://watchtheburn.com/> tai <https://ultrasound.money/>.

⁸² Yogita Khatri 2021: [Staked launches ETH trust that allows users to also earn staking rewards](#). The Block.

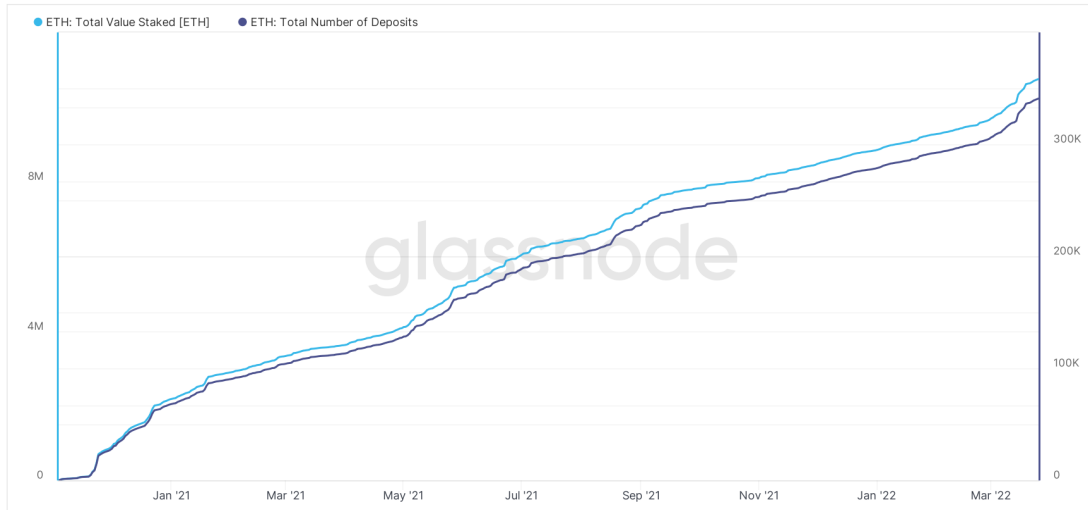
⁸³ Ian Allison 2021: [Banks Edge Closer to Ethereum 2.0 Staking](#). CoinDesk.

⁸⁴ Sam Bourgi 2022: [Crypto Biz: Goldman Sachs tip-toes into ETH, Mar. 4-10](#). Cointelegraph.

⁸⁵ Max Fiege 2019: [Staking-as-a-Service is not a commodity](#). The Block Research.

KUVIO 11. ETHEREUM: ETH2-TALLETUSSOPIMUKSEEN SIIRRETYN ETH:N KOKONAISMÄÄRÄ JA ETH2-PANTTAUSSITOUMUSTEN MÄÄRÄN KEHITYS

ETH: Total Value Staked, ETH: Total Number of Deposits



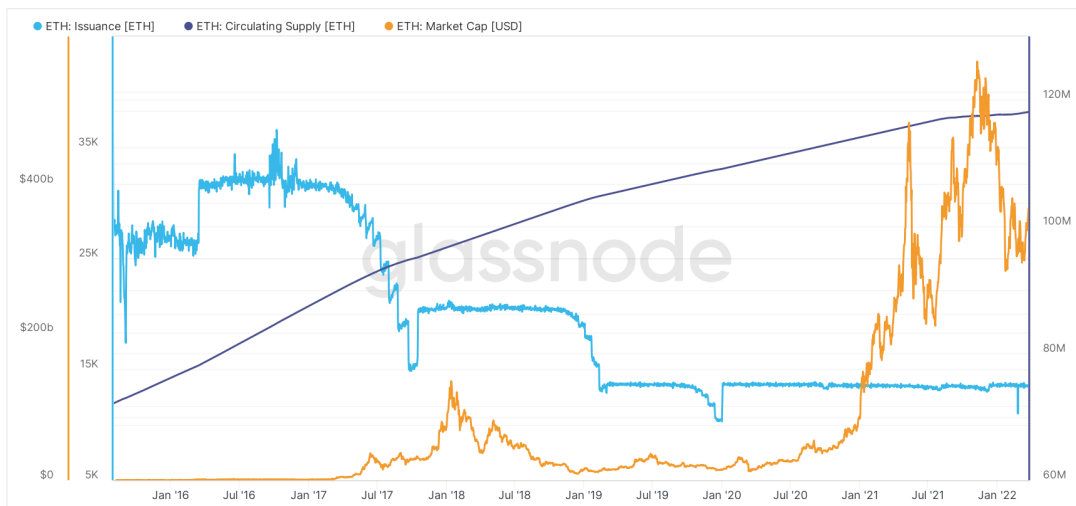
© 2022 Glassnode. All Rights Reserved.

glassnode

Lähde: Glassnode

KUVIO 12. ETHEREUM: MARKKINA-ARVO NYKYTARJONTAAN SUHTEUTETTUNA, KOKONAISTARJONTA JA TARJONTAAN LISÄTYN UUDEN ETH:N MÄÄRÄ

ETH: Issuance, ETH: Circulating Supply, ETH: Market Cap



© 2022 Glassnode. All Rights Reserved.

glassnode

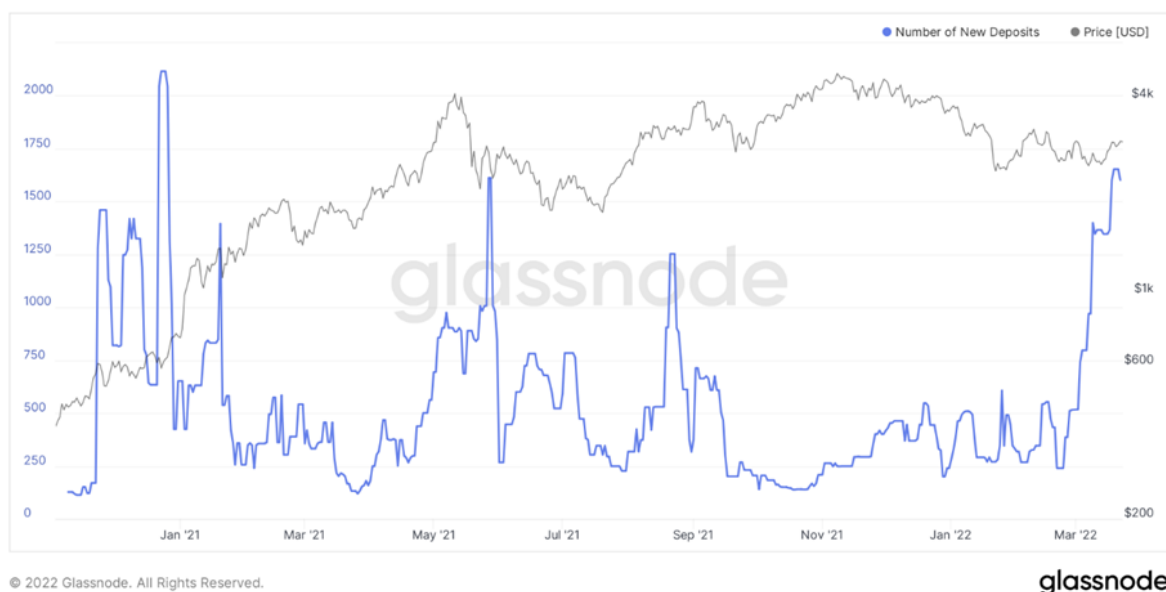
Lähde: Glassnode

ETH-lukitusten määrällinen kasvu ja älysopimukseen sidotun ETH:n kasvanut määrä on huomionarvoista varsinkin siksi, että kukaan ei varmuudella osaa sanoa, milloin PoW- ja PoS-ketjujen sulautuminen tapahtuu (ks. kuvio 13). Tai milloin talletussopimukseen lukittu ETH ja steikkauspalkkio ovat käytettävissä.

Viime kuukausien aikana ETH2-talletussopimukseen lukitun ETH:n kasvanut määrä johtuu todennäköisesti muun muassa siitä, että steikkaustuotot voivat olla jo ennen sulautumista toteutustavasta riippuen jopa 4,3–5,4 % APR. ETH2:ssa mitattuna.⁸⁶ Coinbasen esittämän arvion mukaan sulautumisen jälkeen odotetut steikkaustuotot saattavat olla nykyistä tuotto-odotusta hieman korkeampia (9–12 % APR).⁸⁷

KUVIO 13. ETH2-TALLETUSSOPIMUKSEEN SIIRRETYT UUDET LUKITUT ETH-VARAT

Ethereum: Number of New Deposits (7d Moving Median)



Lähde: Glassnode

ETH:n lukitseminen ETH2-talletussopimukseen saattaa tarjota ETH:n omistajille houkuttelevan tuottomahdollisuuden, mutta erilaisten hajautetun rahoituksen ratkaisujen yleistymisen myötä ETH:n lukitseminen määräämättömäksi ajaksi ei välttämättä kuulosta enää niin houkuttelevalta kuin vielä muutama vuosi sitten. Ne, jotka ovat vakuuttuneita ETH:n ylivertaisuudesta muihin kryptovaluuttoihin ja

⁸⁶ Ethereumin tulevaisuuteen ja steikkaukseen liittyy monenlaisia riskejä ja epävarmuustekijöitä – ja niiden tiedostaminen on tärkeää ennen päätöksentekoa. Ks. esim. David Duong 2022: ETH Staking Post Merge: Yield Estimates and Risk. Coinbase Institutional, 23.2.2022.

⁸⁷ Ks. alaviite 80.

bitcoiniin nähden, *etheriaanit*, eivät välttämättä näe vaihtoehtoiskustannuksia samalla tavoin. Etheriaani saattaa kokea jopa velvollisuudekseen edesauttaa eri keinoin Vitalikin ja kumppanien vision toteuttamista. Tällöin ETH2-talletussopimukseen lukitut ETH-varat tekevät “Herran työtä”.⁸⁸

Lisäksi on hyvä muistaa, että ETH:n lukitseminen ETH2-talletussopimukseen ei vielä tässä vaiheessa tuota validaattorille suoraan lisää ETH:ta. Validaattori saa palkkioksi synteettistä ETH2-tokeneita, ei nykyistä ETH:ta. Kyse on siis siitä, että ETH2:n haltijalla on oikeus, mutta ei varmuutta joskus tulevaisuudessa saada ETH:ta palkkiona liiketoimien vahvistamiseen osallistumisestaan.⁸⁹

Ne, jotka osallistuvat ETH2-talletussopimukseen suoraan tai epäsuoraan, ottavat jo tässä vaiheessa kantaa sekä vanhaan että uuteen Ethereum-lohkoketjuun ja Ethereumin tulevaisuuteen.⁹⁰ ETH:n ja ETH2:n⁹¹ markkinahinnoissa saattaa olla vaihtelua, eikä kryptovaluuttapörssien tuottamia ETH2-tokeneita voi siirtää esimerkiksi kryptovaluuttapörssistä toiseen tai omaan yksityiseen lompakkoon.

Kryptovaluuttapörssit, jotka tarjoavat joko itse tai yhdessä kumppaniensa kanssa ETH2-steikkausta, eivät myöskään välttämättä tarjoa kovin laajaa kaupankäyntiparien valikoimaa ETH2:lle, jonka takia sijoittaja saattaa joutua esimerkiksi maksamaan useampia kaupankäyntikuluja halutessaan muuttaa ETH2:n joksikin muuksi (vrt. ETH2 → ETH → EUR).

Viime kädessä jokaisen ETH:n omistajan on itse päätettävä, miten ja missä vaiheessa hän ottaa kantaa Ethereum-lohkoketjun tulevaisuuteen. ETH:n omistaminen on jo itsessään eräänlainen kannanotto.

Ethereumin – niin kuin myös muiden kryptovaluuttojen ja bitcoinin – tulevaisuuteen liittyy lukemattomia seikkoja, joista osa on laskettavissa ja osa tuntemattomia.

⁸⁸ Henrik Gebbing 2021: [Without staking, institutional crypto investors cannot escape inflation](#). Cointelegraph; Simran Jagdev ym. 2021: [Institutional Staking on Ethereum: One year after the launch of the Beacon Chain](#). ConsenSys Blog.

⁸⁹ Erilaisia ETH-kirjanmerkkejä on useita, esim. Coinbase: [Ethereum 2 \(ETH2 / EUR\)](#), Binance: [Beacon ETH](#)
⁹⁰ Esimerkiksi päätös osallistua ETH2-talletussopimukseen nyt tarjoaa mahdollisuuden lunastaa palkkioksi saadun määrän ETH:ta joskus tulevaisuudessa, jos ETH2 muunnetaan aikanaan ETH:ksi. Päätös olla osallistumatta on hieman monimutkaisempi, koska ETH:n polttojen ansiosta kierrossa olevan ETH:n määrä saattaa hieman vähentyä ajan kuluessa. Niiden ETH:n haltijoiden, jotka eivät osallistu steikkaukseen, ETH-omistukset dilutoituvat eli laimenevat, mikäli kierrossa olevan ETH:n määrä jatkaa (merkittävästi) kasvuaan vielä sulautumisen jälkeenkin (*ceteris paribus*). ETH2-steikkausta voi verrata kärkeästi ETH-merkintäoikeuksien ostamiseen, mutta sillä poikkeuksella, että merkintäoikeuksiin liittyy merkittäviä riskejä, kun lopulliset ehdot ja aikataulut muuttuvat kaiken aikaa.

⁹¹ Lidon ETH2-panttauksen tuottama Lido Staked Ether (stETH) on parempi ja käyttömahdollisuuksiltaan parempi kuin kryptovaluuttapörssien tuottamat ETH2-tokenit, mutta sekään ei ole sama asia kuin ETH. stETH:n ja ETH:n välillä on tällä hetkellä noin 1,5 % preemio ETH:n hyväksi. Lisäksi eri pörssillä ja DeFi-alustoilla saattaa olla laaja valikoima erilaisia ETH2-tokeneita, joiden välillä on hintaeroja, joka saattaa avata kryptosijoittajalle uusia mahdollisuuksia.

Lisäksi on aina mahdollista, että jostain ilmestyy se tuntematon epävarmuus, josta emme edes tiedä, ettemme tiedä niitä.

Miten tästä eteenpäin?

“Rahan internetin [bitcoinin] ei pitäisi maksaa viittä senttiä liiketoimea kohti. Se on jotenkin absurdia.”

– Vitalik Buterin⁹²

Buterinin vuonna 2017 esittämän arvion valossa Ethereumilla on vielä paljon parantamisen varaa: Ethereum-lohkoketjun palkkiot ovat tällä hetkellä monikymmenkertaiset hänen esittämänsä ihanteeseen verrattuna.

Kierrossa olevan ETH:n markkina-arvo on tällä hetkellä noin **340 miljardia euroa** (samaan aikaan ETH:n kierrosta ”poistaminen” jatkuu aiemmin esitettyjen suunnitelmien mukaan) ja yli **105 miljardin euron** arvosta ETH:ta on sidottu erilaisiin hajautetun rahoituksen hankkeisiin. Ethereumin protokollatulot ovat viimeisen 30 päivän aikana olleet noin **275 miljoonaa euroa** ETH:n markkinahinnalla mitattuna.⁹³

Sulautumiseen ja sen jälkeisiin kehitysaskeleisiin on ladattu suuria odotuksia. PoS-siirtymän on *pakko* onnistua Ethereumin arvolupauksen vahvistamiseksi.⁹⁴ Ethereumin parissa työskentelee suuri määrä kehittäjiä (kuvio 13) ja sen ohjelmistokehittäjien ekosysteemi on aktiivinen (kuvio 14). Institutionaalinen kiinnostus kryptovaluuttoja kohtaan on vielä suhteessa pientä, mutta kiinnostus on ollut pienessä nosteessa viime vuosien ajan (ks. kuvio 15).

Ethereumin sulautumisen jälkeinen arvonluontidynamiikka

Hyvin yksinkertaistetusti ETH:n arvonluonti perustuu tulevaisuudessa *oletettuun* PoS-konsensusmallin aikaansaamaan myönteiseen takaisinkytkentään.

1. Sulautuminen tarjoaa ETH:n haltijoille mahdollisuuden lukita ETH:ta haluamansa määrän verkon käyttöön ja ansaita varoille (vaihtelevaa) kryptotuottoa.
 - a. Lukittu ETH tuottaa ”kassavirtaa”
 - b. Validaattorit saavat noin 30 % siirtopalkkioista ”tulona” ja noin 70 % poltetaan (muistuttaen osakkeiden takaisinostamista)
2. Mikäli verkon (Ethereum-lohkoketjun) kysyntä kasvaa, siirtopalkkiot kasvavat ja validaattoreille maksetaan suhteellisesti enemmän palkkiota palkkiona steikkauksesta.
3. Maksetut siirtopalkkiot verkon käytöstä ovat yksi tapa arvioida verkon luomaa arvoa. Ethereumin tapauksessa siirtopalkkioiden fiat-määräinen arvo oli viime vuonna yli 9,8 miljardia dollaria.

Lähde: Kuvio 16 (Bloomberg Intelligence)

⁹² Vitalik Buterin 2017: [Videoleike](#)

⁹³ Token Terminal: [Protocol revenue](#)

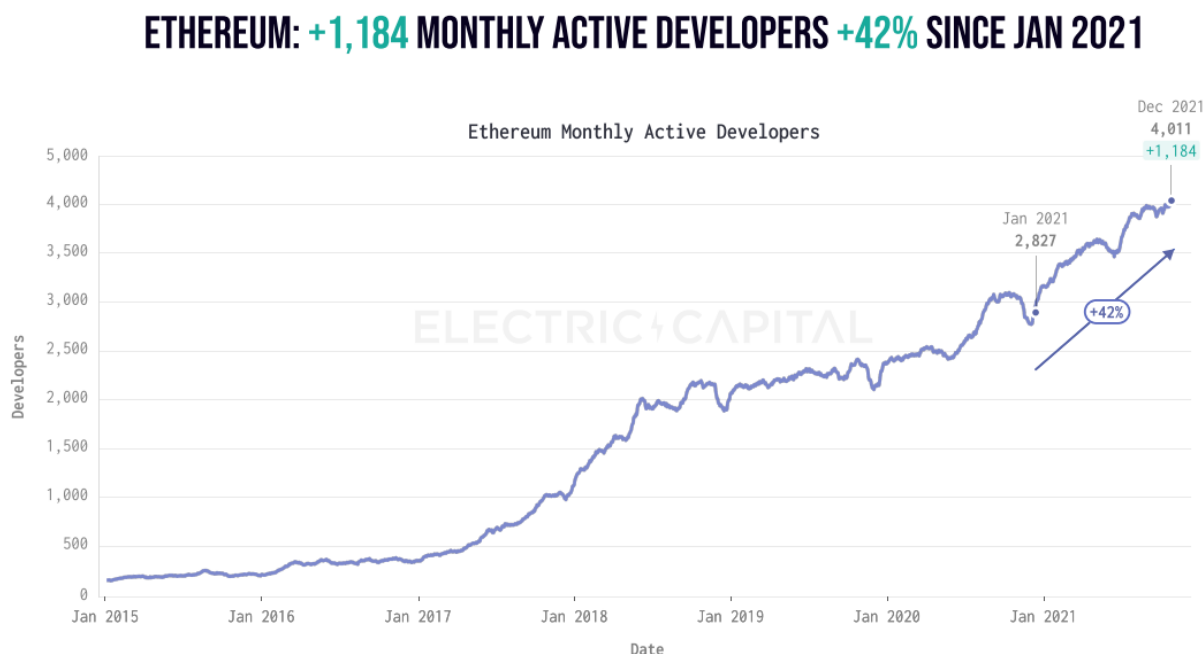
⁹⁴ Ethereum Github: [The Merge Mainnet Readiness Checklist](#)

Ethereumille on muutaman vuoden kuluessa ilmaantunut lukuisia kilpailijoita: Binance Smart Chainin, Avalanche, Fantomin, Solanan, Cardanon, Terran, Algorandin ja Polkadotin kasvuluvut olivat viime vuonna päätä huimaavia. Ne ovat kaikki L1-lohkoketjuja eli Ethereumin suoria kilpailijoita.

Ne ovat toistaiseksi Ethereumia nopeampia, helppokäyttöisempiä ja edullisempia, josta osoituksena muun muassa uusien DeFi-hankkeiden räjähdysmäinen kasvu viime vuonna. Lohkoketjudata osoittaa, että edellä mainittujen uusien L1-ketjujen varaan on rakennettu paljon uutta – ja korkeat siirtokulut ovat olleet eräs keskeinen syy sille, miksi yrittäjät ja kehittäjät ovat rakentaneet uutta niiden varaan Ethereumin sijaan.

Ethereum on suhteellisen hyvin hajautettu lohkoketjuhanke ja heti bitcoinin jälkeen suurin julkinen lohkoketju, mutta sen hallintorakenne ja käyttötapaus on bitcoinista ratkaisevilla tavoin poikkeava.⁹⁵

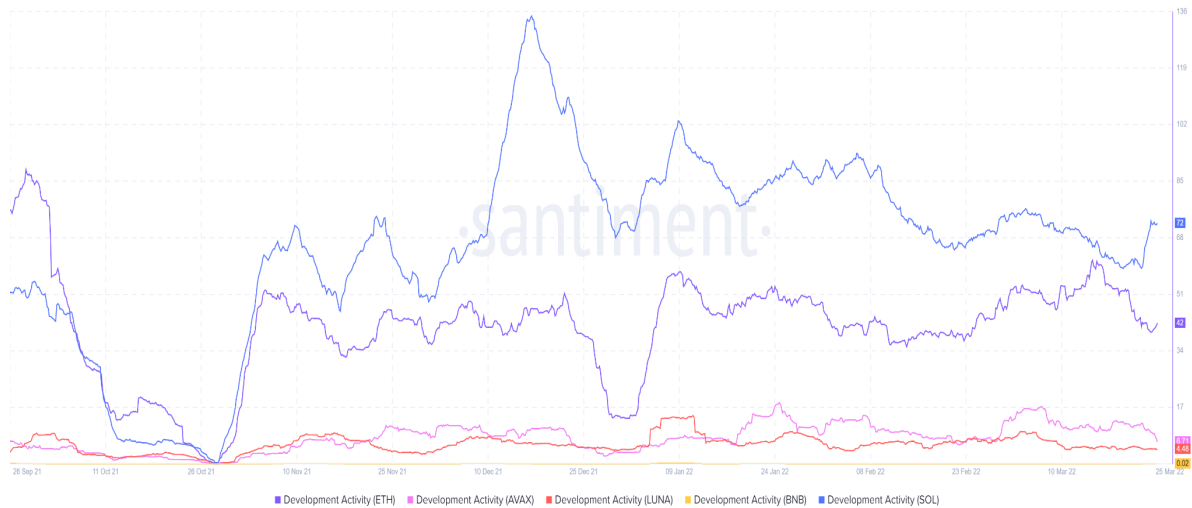
KUVIO 13. ETHEREUMIN KEHITTÄJÄMÄÄRIEN MUUTOS VUOSINA 2015–2021



Lähde: Electric Capital

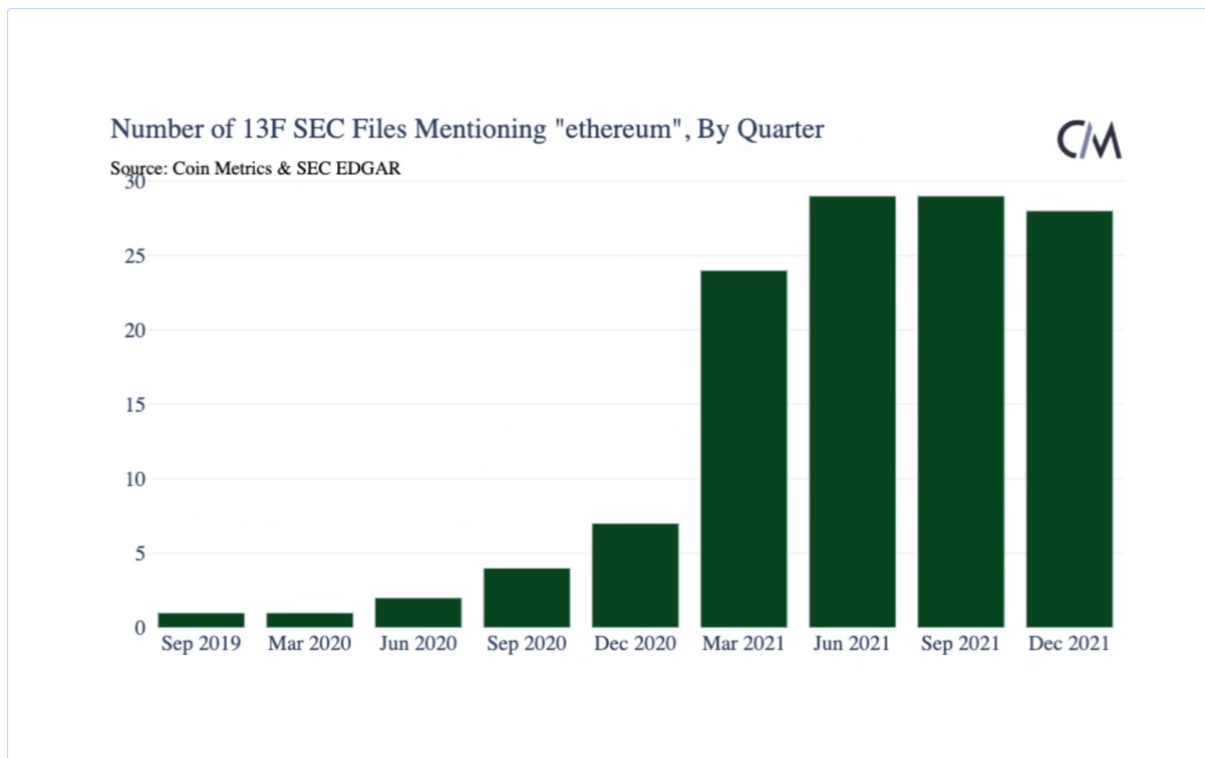
⁹⁵ Pierre Rochard 2018: [Bitcoinin hallinto](#). Brandin kirjasto.

KUVIO 14. ETHEREUMIN KEHITTÄJÄYHTEISÖ ON AKTIIVINEN



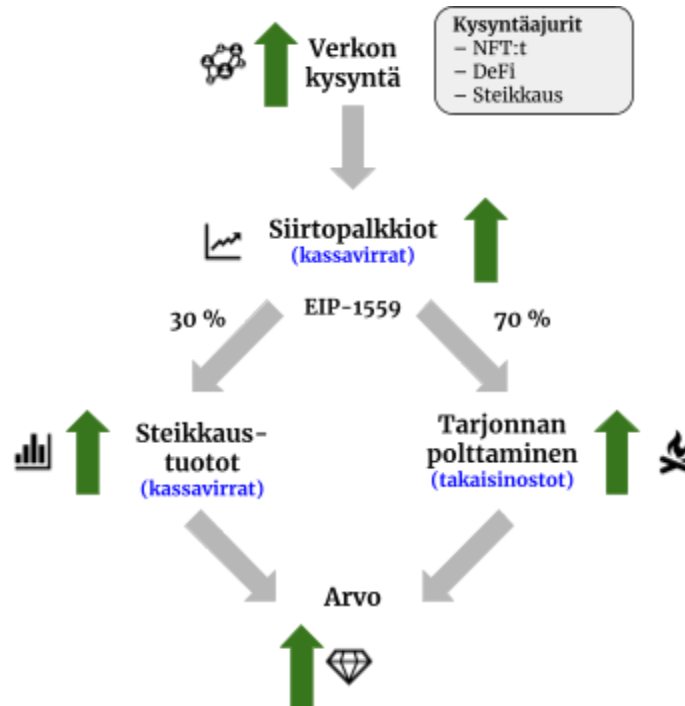
Lähde: Sanbase; Ethereumin kehittäjäyhteisön aktiviteettia kuvaa violetti viiva

KUVIO 15. MAININNAT ETHEREUMISTA SEC:LLE TOIMITETUISSA 13(f)-ILMOITUKSISSA



Lähde: Coin Metrics ([2022](#))

KUVIO 16. ETHEREUMIN YKSINKERTAISTETTU ARVONLUONTIDYNAMIIKKA



Lähde: Bloomberg Intelligence (2022)

Sulautuminen saattaa houkutella uusia käyttäjiä ja kehittäjiä Ethereumin pariin, jos Serenity-vaihteeseen ladatut odotukset onnistutaan lunastamaan. Toki on mahdollista, että Ethereumin asema hallitsevana DeFi- ja NFT-alustana vahvistuu PoS-konsensusmekanismiin siirtymisen yhteydessä entisestään (ks. kuviot 17, 18 ja 19).

Sulautuminen on kauan odotettu tapahtuma, jonka toivotaan parantavan Ethereumin skaalautuvuutta⁹⁶, turvallisuutta ja alentavan merkittävästi siirtokuluja.

Ethereumin parissa työskentelee bitcoiniin verrattuna moninkertainen määrä kehittäjiä ja yrityksiä. Lisäksi Ethereumin varaan on yleiskäyttöisyyden ansiosta rakennettu lukematon määrä muun muassa erilaisia hajautettuja sovelluksia (dApp) kuluneiden vuosien aikana.

⁹⁶ Vitalik Buterin 2021: [Endgame](#). Viime vuoden joulukuussa julkaisemassaan kirjoituksessa Buterin toteaa Ethereum-lohkoketjun koon kasvaneen merkittävästi, joka on aiheuttanut uusia skaalautuvuusongelmia. Täydellistä ratkaisua ei ole olemassa, jonka vuoksi tarvittiin uusi tiekartta Ethereum 2.0:n toteuttamiseksi. Tämä on esitetty Kuviossa.

L1-ketjujen kiristyvistä kilpailusta huolimatta Ethereum on edelleen hallitsevassa markkina-asemassa monilla rintamilla. PoS-konsensusmekanismiin liittyy lukuisia hallinnollisia, taloudellisia ja institutionaalisia muutoksia, jotka muuttavat perustavalla tavalla Ethereumin luonnetta.⁹⁷ Nämä eivät ole vain teknisiä yksityiskohtia, vaan konsensusmallin muuttamiseen liittyy myös useita epävarmuustekijöistä ja tuntemattomia tekijöitä, joista emme edes tiedä, ettemme tiedä niitä.

Tämän vuoden aikana on käytännössä mahdollista seurata lähes reaaliajassa, miten satojen miljardien julkisen arvoverkon avosydänleikkaus suoritetaan lentokoneen lentäessä yläilmoissa ja vauhdin kiihtyessä. Matkan määränpään ja aikataulun piti olla lentokoneeseen noustessa selvä, mutta lukemattomien välilaskujen vuoksi osa matkustajista (ja koneesta poistuneista) pohtii kysymystä, milloin ja mihin matkan aikana muuttuneen lentokone päättyy.

Sus varoitusvarantotodistemallista

[V]arantotodistemalli tuo mukanaan joukon merkittäviä uusia puutteita sekä rahapoliittisiin että hallintomalleihin [työntodisteeseen verrattuna].

Päätelmäni on, että PoS-algoritmit, jotka on toteutettu hajautettuina konsensusmekanismeina lohkoketjuverkkojen protokollakerroksessa, ovat luonteeltaan viallisia kryptojärjestelmiä.

[PoS-järjestelmissä vaaditun ennakkolouhinnan ansiosta kehittäjät] voivat varhaisina osakkaina helposti ylläpitää ja kasvattaa osuuttaan ikuisesti jatkuvan oligopolisen järjestelmän ansiosta, hyötyä plutokratiasta ja ottaa sijoittajat ja pääomasijoittajat varhaisina osallistujina”

KUVIO 17. ETHEREUM: DEFIIN LUKITTU ETH:N NYKYINEN ARVO



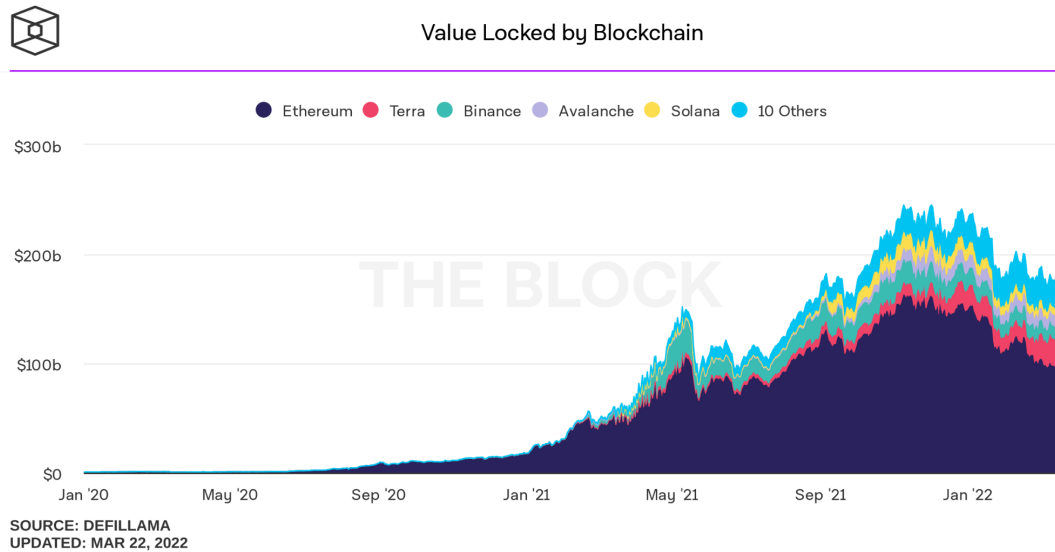
Lähde: Defi Llama

Tämän vuoden aikana on käytännössä mahdollista seurata lähes reaaliajassa, miten satojen miljardien julkisen arvoverkon avosydänleikkaus suoritetaan lentokoneen lentäessä yläilmoissa ja vauhdin kiihtyessä. Matkan määränpään ja aikataulun piti olla

⁹⁷ Vicent Sus 2022: [Proof-of-Stake Is a Defective Mechanism](#).

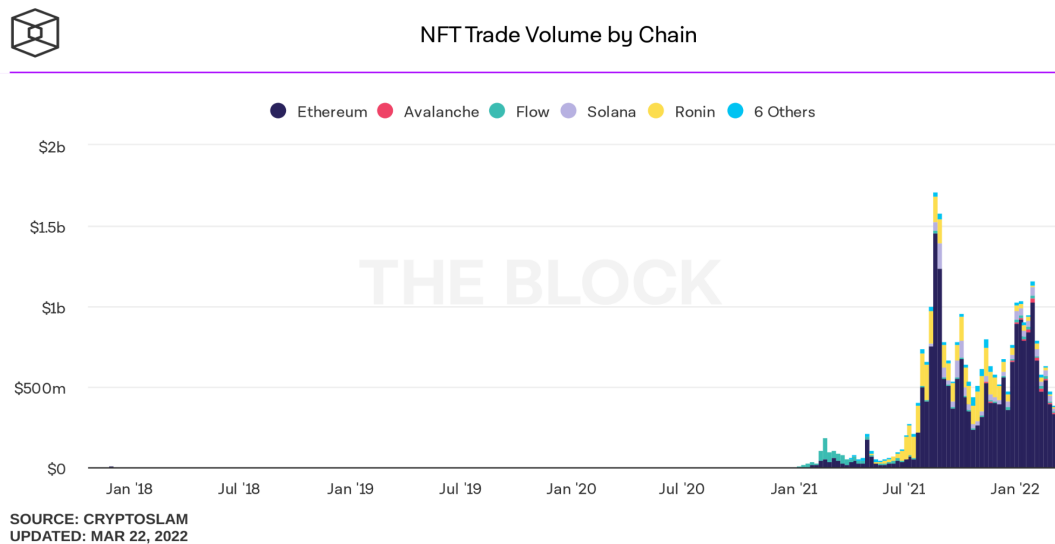
lentokoneeseen noustessa selvä, mutta lukemattomien välilaskujen vuoksi osa matkustajista (ja koneesta poistuneista) pohtii kysymystä, milloin ja mihin matkan aikana muuttuneen lentokone päättyy.

KUVIO 18. ETHEREUMILLA EDELLEEN HALLITSEVA MARKKINA-ASEMA DEFI-LOHKOKETJUNA



Lähde: The Block

KUVIO 19. ETHEREUMILLA ON HALLITSEVA ASEMA NFT-MARKKINOILLA



Lähde: The Block

Kirjoittaja(t):

Thomas Brand

Head of Institutions
Coinmotion

Tärkeää tietoa

Tämä Coinmotion Researchin laatima raportti ("materiaali") keskittyy kryptovaluuttoihin, digitaalisiin varallisuuseriin, avoimiin lohkoketjuihin, rahoitusmarkkinoihin ja/tai finanssiteknologiaan.

Materiaali on laadittu yleisluontoiseksi tiedoksi ja informaatiomateriaaliksi omaan käyttöön niille henkilöille, jotka ovat kiinnostuneita edellä mainituista aihealueista. Historialliset tuotot eivät ole tae tulevasta ja yksittäisen sijoituskohteen hinta voi vaihdella suuresti eri tilanteissa.

Materiaalia ei ole tarkoitettu sijoitussuositukseksi, -neuvonnaksi tai -tutkimukseksi, eikä sitä tule ymmärtää sellaiseksi. Kryptovaluuttoihin, digitaalisiin varallisuuseriin, avoimiin lohkoketjuihin ja vastaaviin sijoittamiseen liittyy merkittäviä riskejä ja epävarmuustekijöitä.

Tavoitteena on antaa mahdollisimman tarkkoja ja oikeita tietoja, mutta Coinmotion ei takaa materiaalissa olevien tietojen täydellisyyttä, soveltuvuutta, täsmällisyyttä, käyttökelpoisuutta tai virheettömyyttä. Materiaaliin kootuissa tiedoissa saattaa ilmetä jatkuvia muutoksia.

Materiaalissa esitetyt tiedot ja arviot voivat muuttua nopeasti, eikä Coinmotion sitoudu päivittämään muutoksia materiaaliin.

Materiaalissa esitetyt kannanotot, näkemykset, kuviot/kaaviot, arviot ja ennusteet on ymmärrettävä niiden esittäneiden mielipiteiksi, eikä niitä voi pitää minkäänlaisena kehotuksena toimeen tai päätökseen. Materiaalin sisältö ei välttämättä vastaa Coinmotionin kulloisiakin näkemyksiä.

Coinmotion Research tai Coinmotion eivät ole vastuussa mistään menetyksistä, vahingoista tai kuluista liittyen tämän materiaalin käyttöön tai materiaalissa olevaan tai siitä mahdollisesti puuttuvaan informaatioon liittyen.

Don't trust. Verify.

Päivämäärä

31. maaliskuuta 2022

Palaute ja yhteydenotot

institutions@coinmotion.com



Coinmotion Oy
Kauppakatu 39
40100 Jyväskylä
Y-tunnus 2469683-1