Valtteri Peltoniemi

Kryptovaluutat - onko Ethereumista Bitcoinin haastajaksi

Tietotekniikan kandidaatintutkielma

10. kesäkuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Valtteri Peltoniemi

Yhteystiedot: vamipelt@student.jyu.fi

Ohjaaja: Tuomo Rossi

Työn nimi: Kryptovaluutat - onko Ethereumista Bitcoinin haastajaksi

Title in English: Cryptocurrencies - whether Ethereum is a contender for Bitcoin

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 29+0

Tiivistelmä:

Kryptovaluutat on jo monelle ihmiselle tuttu käsite, mutta teknologia niiden takana ei välttämättä vielä ole. Uutisissa vilahtelee entistä useammin kryptovaluuttoja ja niiden suuria arvon nousuja. Kryptovaluuttojen arvo on noussut merkittävästi loppuvuodesta 2020 lähtien. Tässä tutkielmassa esitellään kryptovaluuttojen toimintaa keskittyen erityisesti Bitcoiniin ja Ethereumiin. Tutkielman tarkoituksena on selvittää onko Ethereumista Bitcoinin haastajaksi lohkoketjun tuomilla ominaisuuksilla, sillä molemmat kryptovaluutat ovat selvästi markkina-arvollisesti muita edellä keväällä 2021.

Avainsanat: Bitcoin, Ethereum, kryptovaluutta, lohkoketju

Abstract:

Cryptocurrencies are already a familiar concept to many people, but the technology behind them might not be. The news are reporting more about cryptocurrencies and their huge increase in value since end of 2020. This thesis examines how cryptocurrencies are working and focuses especially on Bitcoin and Ethereum. The purpose of this thesis is to study if Ethereum can challenge Bitcoin with the blockchain features, as both cryptocurrencies are clearly ahead of the others in terms of market value in the spring of 2021.

Keywords: Bitcoin, Ethereum, cryptocurrency, blockchain

Kuviot

Sisällys

1 Johdanto

Kryptovaluutat voidaan jakaa neljään erilaiseen tyyppiin, joita ovat stablecoins, hallinnollinen tokeni (governance tokens), turhat kolikot (shit coins) ja keräiltävät tokenit (collectible tokens). Stablecoinit ovat kolikoita, jotka peilaavat perinteisen valuutan arvoa kuten euron arvoa. Tämä ratkaisee monien kryptovaluuttojen epävakausongelman. Hallinnolliset tokenit on tarkoitettu tunnuksiksi, jotka edustavat äänioikeutta hajautetussa organisaatiossa. Turhiksi kolikoiksi lasketaan kolikot, jotka on tehty huvin vuoksi tai meemiin perustuen. Kryptovaluutan voi luoda kuka tahansa, jolloin valuuttojen joukkoon syntyy sellaisia valuuttoja, joilla ei ole mitään tarkoitusta, esimerkiksi Dogecoin. Keräiltävät tokenit ovat tunnuksia, jotka edustavat jotain keräiltävää tai ainutlaatuista omaisuutta, esimerkiksi pelituote tai digitaalinen taide. Nämä tokenit tunnetaan yleisesti nimellä NFT (non-fungible tokens) (Ethereum.org 2021b).

Kryptovaluuttoista tunnetuin sekä arvoikkain on Bitcoin. Sitä haastamaan on luotu paljon valuuttoja, mutta tähän kirjallisuuskatsaukseen olen valinnut Ethereumin, joka mielestäni on potentiaalinen tulevaisuuden kilpailija ja toiseksi suurin kryptovaluutta markkina-arvoltaan keväällä 2021. (CoinMarketCap 2021) Tämän kandidaatin tutkielman tarkoituksena on selvittää, voisiko Ethereum olla Bitcoinia parempi lohkoketjun tuomilla ominaisuuksillaan, vaikka sen arvo onkin pienempi kuin Bitcoinin. Työn 2 luvussa kerrotaan yleisesti kryptovaluutan historiasta, lohkoketjun toiminnasta ja ominaisuuksista. Kryptovaluuttojen pintaraapaisun jälkeen keskitytään syvemmin tässä tutkielmassa käsiteltäviin kryptovaluuttoihin, eli Bitcoiniin ja Ethereumiin. Luku 3 kertoo Bitcoinista ja luku 4 puolestaan Ethereumista. Molemmista valuutoista käydään läpi syntyhistoriaa, erityistietoa lohkoketjun toiminnasta ja lopuksi ominaisuuksia. Viidennessä luvussa kerrotaan, mistä kryptovaluutat saavat arvonsa ja mitkä asiat siihen vaikuttavat. Tämän jälkeen luvussa 6 vertaillaan Bitcoinin ja Ethereumin eroja ja yhteenvedossa kasataan aiemmissa luvuissa esitettyjä tietoja ja pohditaan, miten löydetyt erot vaikuttavat kryptovaluuttojen tulevaisuuteen.

2 Kryptovaluutta

Finansivalvonta (2019) määrittelee kryptovaluutan olevan virtuaalivaluutta, joka käyttää salausalgoritmiikkaa. Ensimmäinen kryptovaluutta Bitcoin perustettiin vuonna 2008, mutta vasta viime vuosina kryptovaluuttojen määrä on lähtenyt suureen kasvuun. Best (2021) mukaan helmikuussa 2021 kryptovaluuttoja oli yhteensä 4501.

Royal ja Voigt (2021) toteavat kryptovaluutan olevan maksumuoto, jota käyttäjä voi vaihtaa tavaroihin ja palveluihin. Monet yritykset ovat laskeneet liikkeelle oman valuutan, jota kutsutaan tokeniksi. Niillä on tarkoitus käydä kauppaa nimenomaan yrityksen tarjoamaa tuotetta tai palvelua vastaan. Kryptovaluutoissa käyttäjän on vaihdettava todellista valuuttaa kryptovaluuttaan.

2.1 Historia

Ajatukset kryptovaluutasta syntyivät 10 vuotta ennen ensimmäisen kryptovaluutan syntymistä. Vuonna 1998 tietokoneinsinööri Wei Dai julkaisi raportin kryptovaluutasta, jonka hän nimesi B-Money:ksi. Hänen ajatuksissaan B-Money oli digitaalinen valuutta, jota voitaisiin lähettää muille. Valuutan lähetys tapahtuisi jäljittämättömien digitaalisten salanimien mukana. Myöhemmin samana vuonna Nick Szabo yritti luoda Bit Gold nimisen kryptovaluutan. Szabon tavoitteena oli luoda hajautettu digitaalinen valuutta. (ledger.com 2019).

Ensimmäistä kryptovaluuttaa Bitcoinia varten luotiin myös kryptovaluuttapörssejä, jotta Bitcoinilla pystyttäisiin myös käymään kauppaa. Maaliskuussa 2010 perustettiin Bitcoinmarket.com ja siitä tuli ensimmäinen kryptovaluuttapörssi. Samana vuonna se sai kilpailijan nimeltä Mt. Gox. Tästä alkoi Bitcoinin arvon kasvaminen ja vuosien 2011–2013 aikana se saavutti samanarvoisuuden Yhdysvaltain dollarin kanssa. Kiinnostus Bitcoinia kohtaan sai myös muut kehittämään uusia kryptovaluuttoja ja toukokuussa 2013 kryptovaluuttamarkkinoilta löytyi jo 10 kryptovaluuttaa, joista tunnetuimpia ovat Litecoin ja XRP. (ledger.com 2019).

Bitcoinin arvon nousun myötä alkoivat myös hakkeroinnit kryptovaluuttojen perään. Mt. Gox joutui hakkeroinnin kohteeksi kesäkuussa 2011, jolloin hyökkääjä sai varastettua itsel-

leen 2000 Bitcoinia. Hakkerointi ei kuitenkaan vielä vaikuttanut Mt. Goxin suosioon, sillä siitä tuli suurin kryptovaluuttapörssi vuonna 2013. Kuitenkin Mt. Goxia kohtasi toinen hakkerointi, kun vuonna 2014 kryptovaluuttapörssistä varastettiin 850 000 Bitcoinia. Tämä on Bitcoinin historian suurin varkaus, jonka arvo oli tuolloin 460 miljoonaa dollaria eli nykyarvolla yli 48 miljardia dollaria (5.4.2021). Tämän Bitcoinin historian suurimman hakkeroinnin jälkeen sen arvo tippui 50 prosenttia. Kryptovaluuttapörssien hakkerointeja on tapahtunut Mt. Goxin jälkeenkin, mutta harvoin sen suuruusluokassa. (ledger.com 2019).

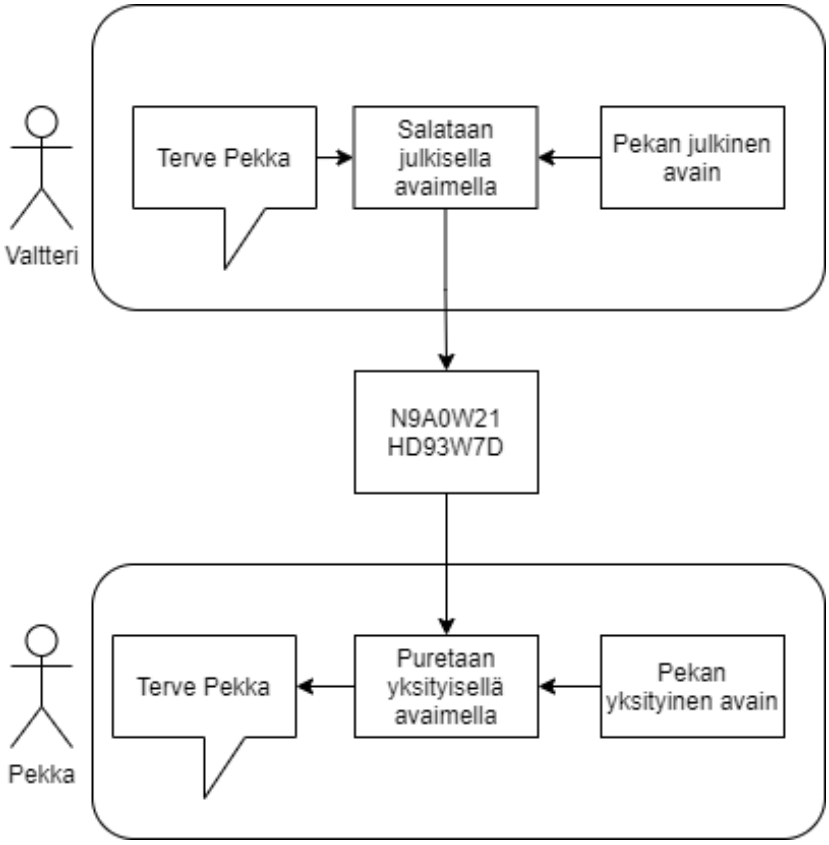
2.2 Kryptovaluuttojen toimintamekanismi

Ensimmäisen lohkoketjun kehittäjä Satoshi Nakamoto käytti Bitcoinin white book:ssa nimeä chain of block, mutta myöhemmin vuonna 2015 nimeksi tuli blockchain. Lohkoketjun toiminta on karkeasti niinkin yksinkertainen, että transaktioita tallennetaan jatkuvana syöttönä lohkoon. Niitä ei laiteta sinne yksitellen, vaan transaktiot kasataan lohkoksi, johon mahtuu tietty määrä dataa. Sen jälkeen, kun lohko on täynnä dataa sen sisältö varmistetaan ja lohko on valmis yhdistettäväksi muihin lohkoihin. Yhdistäminen tai linkittäminen tapahtuu kryptokraafisilla salausmenetelmillä edelliseen lohkoon. Tällä tavalla syntyy linkitettyjen lohkojen ketju eli lohkoketju (Johansson ym. 2019a).

Kryptovaluutat perustuvat lohkoketjuteknologiaan. Se on mahdollisesti ihmiskunnan suurin keksintö sitten Internetin. Lohkoketjuteknologian avulla lohkoketjun eri osapuolet pystyvät luomaan ja ylläpitämään hajautettuja ja jaettuja tietokantoja. Lohkoketjua voidaan kutsua myös eräänlaiseksi tilikirjaksi, jota jaetaan vertaisverkkoon (peer-to-peer) kuuluvien tahojen kesken (Acharjamayum, Patgiri ja Devi 2018). Lohkoketjut tarjoavat ihmisille paljon erilaisia hyötyjä, joista suurimpia ovat ehdottomasti turvallisuus ja luotettavuus. Lohkoketjuteknologia mahdollistaa lukuisat kryptovaluuttojen mukanaan tuomat hyödyt, joista kerrotaan lisää myöhemmin (Northcrypto.com 2018) .

Lohkoketjujen toiminnassa on mukana julkisen avaimen salaus eli PKI (public key infrastructure). Julkisen avaimen salaus perustuu identiteetin todistamiselle elektronisessa maailmassa. Fyysisessä maailmassa käytetään passeja tai henkilökortteja itsensä todistamiseen. PKI perustuu kahteen avaimeen: julkiseen ja yksityiseen. Julkinen avain on nimensä mu-

kaisesti julkinen, kaikkien nähtävillä oleva avain. Yksityisen avaimen tarkoituksena on olla henkilökohtainen, visusti omana tietona pidettävä. Avainten ideana on, että niillä voi tehdä lähetettävästä tiedostosta tai viestistä salaisen. Esimerkiksi lähetettäessä jollekkin tiedostoa, tiedosto lähetetään henkilön julkiseen avaimeen, joka muuttaa tiedoston salatuksi. Tämän salauksen pystyy purkamaan ainoastaan vastaanottavan henkilön yksityinen avain. Tämä tarkoittaa sitä, että kukaan välikäsi ei pysty tutkimaan tiedostoa lähettäjän ja vastaanottajan välillä (Johansson ym. 2019b).



Kuvio 1. PKI avainten käyttö transaktiossa (Mooter 2020) mukaisesti kuvattuna

Lohkoketjun tiedot sijaitsevat tilikirjassa eli ledgerissä. Tämä tapahtumarekisteri sijaitsee lohkoketjun ytimessä, jonne kaikki suoritetut transaktiot on tallennettu. Tilikirjan tietoja pystytään katsomaan eri toimijoiden toimesta reaaliaikaisesti (Johansson ym. 2019c). Lohkoketjun muuttamiseen tarvitaan kaikkien toimijoiden enemmistön hyväksyntä. Tätä yhteisymmärrystä kutsutaan konsensukseksi. Kun muutos on saanut enemmistön hyväksynnän, kaikki tietokoneet päivittävät automaattisesti kopionsa tilikirjasta samanaikaisesti. Jos tili-

kirjaa yritetään muuttaa ilman oikeaa versiota, niin muut koneet hylkäävät sen virheellisenä (Johansson ym. 2019d).

Lohkoketju toimii hajautetusti eri osapuolten välillä. Tämä aiheuttaa lohkoketjulle konsensusongelman eli kuinka kaikki lohkoketjuun osallistuvat osapuolet saadaan yhteisymmärrykseen oikeasta tilasta. Konsensusalgoritmin tehtävänä on pitää lohkoketju toiminnassa ja ratkaista konsensusongelma. Tämä ratkaistaan matemaattisesti todistettavalla tehtävällä eli jollain konsensusalgoritmilla. Tällöin luottamusta muihin osapuoliin ei tarvita. Konsensusalgoritmejä ovat muun muassa PoW, PoS, BFTA ja DPos. Tässä tutkielmassa keskitytään ainoastaan POW- ja POS-konsensusalgoritmeihin (Johansson ym. 2019d).

Lohkoketjun osapuolia kutsutaan louhijoiksi, jotka ovat lohkoketjun ylläpitäjiä. Louhijat ovat todella tehokkaita tietokoneita, jotka kilpailevat matemaattisten yhtälöiden eli konsessusalgoritmin ratkaisemisesta. Ensimmäisenä yhtälön ratkaissut pääsee luomaan uuden lohkon kyseiseen lohkoketjuun. Tästä hyvästä louhija saa louhintapalkkion, joka on lohkoketjun sisään ohjelmoitu ominaisuus, joka säätelee kryptovaluuttojen syntymistahtia. Louhintapalkkion lisäksi louhijat saavat osuuden kyseisessä lohkoketjussa suoritettujen transaktioiden seurauksena maksetuista transaktiomaksuista (Northcrypto 2018) (Nair ja Dorai 2021).

Kryptovaluutan louhinta voidaan jakaa kahteen osaan: PoW- ja PoS-louhintaan. Proof of Work (PoW) -konsensusalgoritmin toiminta perustuu datan työmäärään. Ideana on, että datan generoimiseen vaaditaan tietokoneelta tietty määrä laskentatehoa. Tehomäärän pitää olla sopiva, jolloin se ei ole liian helppo hyökkääjälle, mutta ei taas liian suuri louhijalle. Tehomäärän ollessa sopiva, hyökkääjän on kannattamatonta hyökätä louhijaverkkoa vastaan, sillä vaadittu työmäärä on tavoitteisiin nähden turhan suuri. Proof of Work -konsensusalgoritmissa kryptovaluutat vaativat toimiakseen louhijoiden fyysistä työtä. Kryptovaluutta ei siis toimi kunnolla, jos sillä ei ole louhijoita koko ajan louhimassa lohkoja (Kryptovaluutta.fi 2021) (Nair ja Dorai 2021).

Proof of Stake (PoS) -louhintamallin ajatuksena on, että henkilö voi kaivaa tai vahvistaa lohkotapahtumia sen perusteella, kuinka paljon hänellä on kyseisen valuutan kolikoita. PoS luotiin vaihtoehdoksi PoW:lle, joka kuluttaa valtavan määrän energiaa johtuen työn määrästä. Proof of Stake -toiminnassa louhinta perustuu prosentuaaliseen osuuteen. Esimerkiksi jos

Bitcoin toimisi Proof of Stake -konsensusalgoritmilla, tämä tarkoittaisi sitä, että jos louhija omistaisi neljä prosenttia kaikista saatavilla olevista Bitcoineista, niin tällöin hän pystyisi louhimaan neljä prosenttia lohkosta. Proof of Stake -järjestelmä on yhtä turvallinen tai jopa turvallisempi kuin Proof of Work -järjestelmä. Proof of Stake -mallissa hyökkääjän on saatava haltuunsa enemmistö kyseisen valuutan kolikoista eli 51 prosenttia. Ilman enemmistöosuutta kryptovaluutasta, hyökkääjä ei saa tehtyä virheellistä lohkoa lohkoketjuun. Enemmistön osuuden saaminen vaatisi suurta rahallista panostusta ja mikäli valuutan arvo laskisi, menettäisi hyökkääjä myös käyttämänsä varat (Frankenfield 2019) (Nair ja Dorai 2021).

2.3 Ominaisuudet

Lohkoketjuja jaetaan erilaisiin sukupolviin sen kehittymisen perusteella (Reiff 2020). Iredale (2020) ja Northcrypto.com (2018) artikkeleissa todetaan että kryptovaluutan ominaisuudet tulevat lohkoketjuteknologiasta, jota kyseinen kryptovaluutta käyttää. Heidän mukaansa ensimmäisen sukupolven lohkoketjun tuomia ominaisuuksia ovat muun muassa muuttumattomuus, hajautus, turvallisuus, yksimielisyys ja nopeammat transaktiot

Lohkoketjujen mahdollisesti suurin ominaisuus on se, että lohkoketjua ei hallinnoi mikään yksittäinen taho, vaan se on monen tietokoneen muodostama itsenäinen verkko. Tämä antaa lohkoketjun tiedoille turvan siitä, ettei kukaan pysty muuttamaan tietoja lohkoketjun sisällä, ellei sillä ole enemmistöä takanaan. (Johansson ym. 2019e) Kryptovaluuttojen turvallisuus tulee erityisestä salauksesta, jota sovelletaan käyttäen kahta salauksen pääelementtiä - hajautusta ja digitaalisia allekirjoituksia. Hajautus varmistaa tietojen eheyden, ylläpitää lohkoketjun rakennetta ja koodaa ihmisten tilien osoitteet ja tapahtumat. Se tuottaa salauspalapelit, joiden avulla louhiminen on mahdollista. Digitaalisten allekirjoitusten avulla henkilö voi todistaa omistavansa salatun tiedon, paljastamatta kyseisiä tietoja. Kryptovaluutoissa tätä tekniikkaa käytetään rahasiirtojen allekirjoittamiseen. Se todistaa verkolle, että tilinomistaja on suostunut tapahtumaan (cmcmarkets.com 2021).

Lohkoketju on hajautettu, julkinen luettelo kryptovaluutan tapahtumista. Valmiit lohkot, jotka koostuvat uusimmista tapahtumista, tallennetaan ja lisätään lohkoketjuun. Ne tallennetaan aikajärjestyksessä avoimena, pysyvänä ja todennettavana tietueena. Vertaisverkon käyttäjät

hallitsevat lohkoketjua ja noudattavat asetettua protokollaa uusien lohkojen vahvistamiseksi. Jokainen verkkoon liitetty solmu tai tietokone lataa automaattisesti kopion lohkoketjusta. Tämä antaa kaikille mahdollisuuden seurata tapahtumia ilman keskitettyä kirjanpitoa (cmcmarkets.com 2021).

Toisen sukupolven lohkoketjuiksi kutsutaan lohkoketjuja, joilla pystyisi tekemään älykkäitä sopimuksia (Reiff 2020). Älykäs sopimus on periaatteessa vähintään kahden eri osapuolen välinen digitaalisesti allekirjoitettu ja laskennallisesti toteutettava sopimus. Sopimuksen ei ole pakko olla pelkästään koodia, vaan se voi sisältää myös luonnollista kieltä. Lohkoketjuun laitettava sopimus sisältää myös ohjelmistoagentin, joka valvoo sopimusta ja voi suorittaa sopimuksen ilman ihmisen toimintaa (Johansson ym. 2019f).

3 Bitcoin

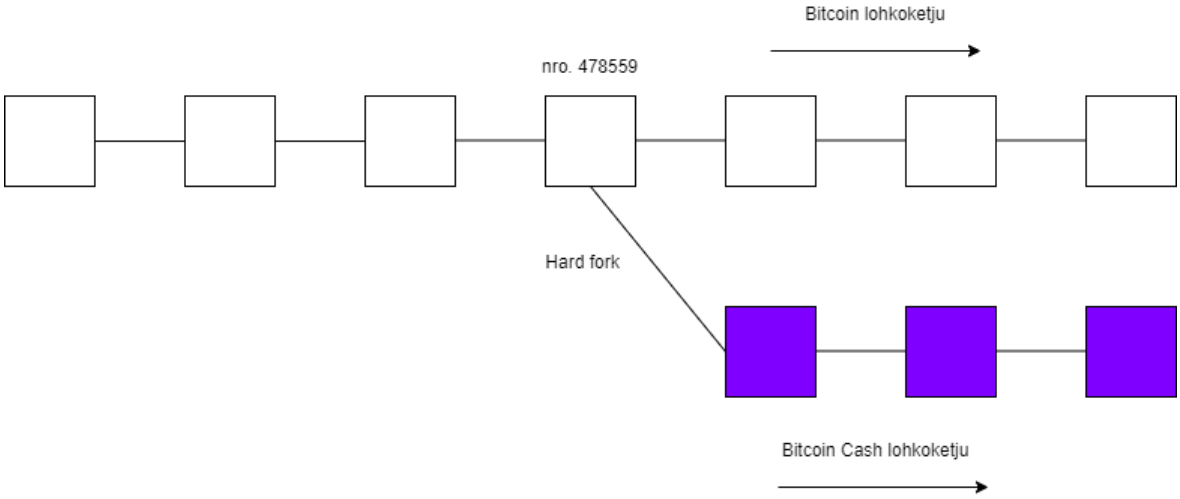
Bitcoinia ei suunniteltu olemaan mitään muuta kuin alusta virtuaalisten arvomerkintöjen kirjaamiselle. Nykyään maailmassa on monta kryptovaluuttaa, jotka ovat lähes samanlaisia lohkoketjultaan kuin Bitcoin, mutta sisältävät pieniä teknisiä muutoksia, jotka näkyvät valuutan ominaisuuksissa. Tällaisia ovat lohkojen sisältämien transaktioiden määrä tai lohkojen luontinopeus. Ensimmäisen sukupolven lohkoketjuun lasketaan sellaiset valuutat, joiden ainoana tehtävänä on olla virtuaalivaluutta (Johansson ym. 2019g). Tässä luvussa käsitellään ensimmäisen sukupolven lohkoketjun omaavaa Bitcoinia, joka aloitti kryptovaluuttojen sisäänmarssin olemassa ololaan.

3.1 Syntyperä

Satoshi Nakamoto julkaisi 2008 kryptosalauksesta kiinnostuneiden ihmisten sähköpostilistalle white paper:n nimeltä Bitcoin: Peer-to-Peer Electronic Cash System, joka kuvaa Bitcoin-lohkoketjuverkoston toimivuutta. (Bonneau ym. 2015) Nakamoto pohdiskeli White paper:ssa, että tällä hetkellä nettikaupat toimivat kolmannen osapuolen varassa maksujen suhteen. Kuitenkin maksutoimintaan liittyy paljon epävarmuutta ja heikkouksia. Maksuja pystytään peruuttamaan ja petoksia tapahtuu. Tähän Nakamoto ehdotti sähköistä maksujärjestelmää, joka perustuu salaustodistukseen luottamuksen sijasta ja osapuolet voivat käydä kauppaa keskenään ilman kolmatta osapuolta. Bitcoin-kryptovaluutta syntyi ajatuksesta tarjota luotettava rahansiirto mahdollisuus kaikille ihmisille (Nakamoto 2008). Neljä kuukautta myöhemmin Satoshi Nakamoto kaivoi Bitcoin-verkon ensimmäisen lohkon, joka tunnetaan myös nimellä Genesis Block. (Bonneau ym. 2015)

Bitcoinin päivittyessä sen historiassa on tapahtunut useita hard forkeja, mikä tarkoittaa radikaalia muutosta lohkoketjuverkon protokollaan. Näistä tunnetuin on mahdollisesti Bitcoinin jakautuminen Bitcoiniksi ja Bitcoin Cashiksi (Peters 2021) (Hou ja Chen 2020). Bitcoinin kehittäjät alkoivat keskustella Bitcoinin tehokkuuden nostamisesta. Bitcoinin yksi lohko on rajoitettu yhteen megatavuun. Tähän kehittäjillä oli erilaisia visioita. Osa halusi kasvattaa lohkon fyysistä kokoa ja osa taas halusi kasvattaa lohkon kokoa salamaverkon avulla. Tä-

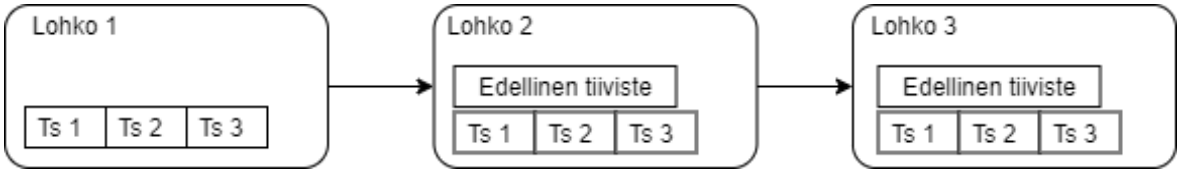
mä keskustelu päättyi elokuussa 2017, jolloin Bitcoin otti käyttöönsä SegWit-salamaverkon. Tällöin lohkon koon kasvattamista kannattanut joukko erosi omaksi ryhmäkseen ja Bitcoin jakautui kahdeksi eri virtuaalivaluutaksi lohkon 478559 kohdalla (Hyppänen 2020a).



Kuvio 2. Esimerkkikuva Bitcoin ja Bitcoin cash hard fork:sta

3.2 Lohkoketjun toiminta

Bitcoin-lohkoketju pitää sisällään lohkoista koostuvan ketjun, joka on järjestykseltään kronologinen. Lohko voi pitää sisällään mitä tahansa merkkijonoja, ykkösiä ja nollia, jotka voivat olla esimerkiksi sähköposteja, todistuksia tai mitä tahansa kahden osapuolen välisiä sopimuksia, mutta Bitcoinin tapauksessa se sisältää vain luetteloa Bitcoinin transaktioista (Floyd 2020). Kuviossa 3 on esimerkki Bitcoin-lohkoketjusta. Esimerkissä yksi lohko pitää sisällään tilikirjan kolmesta tapahtumasta, jotka on merkitty Ts:nä. Lohkojen välinen salaus on suoritettu tiivisteellä (hash). Tiiviste on algoritmi tietojen eheyden vahvistamiseksi. Tiiviste pitää sisällää arvon edellisen lohkon sisällöstä. Tämä arvo on siis epämääräinen kasa numeroita ja kirjaimia (Mooter 2020) (Acharjamayum, Patgiri ja Devi 2018).



Kuvio 3. Bitcoin lohkoketjun toiminta suomennettu (Mooter 2020) kuvasta

Nykyään louhijat ovat järjestäytyneet altaiksi (pool). Tämä parantaa menestymismahdollisuuksia jakamalla laskentatehon ja palkkiot keskenään (Bonneau ym. 2015). Jos yksittäinen kaivospooli on suurempi kuin 50 prosenttia verkon kaivosvoimasta, voivat sen jäsenet hallita transaktioita mielensä mukaan. Yksittäinen transaktio vaatii louhijoilta todistuksen oikeellisuudestaan, mutta enemmistöllä yksittäinen taho voi myös valheellistaa transaktion(Acharjamayum, Patgiri ja Devi 2018). Vuonna 2014 Gash.io saavutti 51 prosenttia Bitcoinin verkon laskentatehosta. He kuitenkin vapaaehtoisesti pienensivät tehon 39.99 prosenttiin, jotta tämä ei vaikuttaisi Bitcoinin hajautukseen ja luottamukseen sen arvosta (Floyd 2020).

Bitcoinin louhinta toimii karkeasti siten, että full node -palvelimet pitävät hallussaan koko Bitcoin-lohkoketjua. Louhijat poimivat transaktioita mempool-nimisestä säiliöstä ja kokoavat ne yhdeksi lohkoksi. Mempool sisältää kaikki transaktiot, jotka on todettu sääntöjen mukaisiksi. Louhinnan tarkoituksena on taata siirtojen pysyvyys ja luoda pysyvä tallenne niiden keskinäisestä järjestyksestä. Tämä on toteutettu määrittelemällä lohkon tiivisteelle tietyt ehdot. Uusi hyväksytty lohko löytyy, kun louhija saa laskettua lohkon tiivisteen ehdot onnistuneesti. Näistä ehdoista saadaan myös säädettyä lohkon löytämiseen vaadittavan laskennan haastavuus eli määrä. Lohkoketju muodostuu lohkoista, joissa uusin lohko sisältää edellisen lohkon tiivisteen. On mahdollista, että lohkoketju lähtee haarautumaan kahdeksi haaraksi. Tällöin se haara jää voimaan, jonka laskennallinen haastavuus on isompi (Kryptovaluutta.fi 2021).

3.3 Ominaisuudet

Bitcoin.org (2021) listaa Bitcoinin ominaisuuksien olevan maksuvapaus, palkkioiden määrän vapaus, turvallisuus ja hallinta sekä läpinäkyvyys. Bitcoin on maksuvapaa, mikä tar-

koittaa sitä, että pystyt lähettämään ja vastaanottamaan Bitcoineja milloin ja missä tahansa. Bitcoinien lähettämisestä peritään lähetysmaksu, joka on lähettäjän itse valittavissa. Palkkiot eivät liity siirrettävään määrään, joten ei ole väliä paljonko Bitcoineja siirrät. Suuremmilla palkkioilla saa transaktion tapahtumaan nopeammin, sillä louhijat priorisoivat maksuja sen mukaan mitä suurempi palkkio on (Bitcoin.org 2021).

Bitcoinin tapahtumat ovat peruuttamattomia eivätkä sisällä asiakkaiden henkilökohtaista sisältöä (Bitcoin.org 2021). Tapahtumien peruuttamattomuus perustuu kuviossa 3 esitettyyn tiivisteeseen ja sen toimintaan. Jos esimerkiksi lohkon 1 Ts1 tapahtumaa muutettaisiin, niin lohkoketjun syntymisen jälkeen lohkon 2 tiiviste huomaisi, että sillä oleva tiiviste ei enää pidä paikkaansa. Jos lohkon 2 tiiviste muokattaisiin myös oikeaksi, lohkon 3 tiiviste huomaisi puolestaan eron siinä, että lohkon 2 tiivistettä on muokattu. Yhden lohkon muuttaminen ei ole mahdollista sillä samalla pitäisi muuttaa joka ikinen lohko kyseisestä lohkosta eteenpäin (Mooter 2020). Muuttumattomuus suojaa kauppiaita petosten tai vilpillisten takaisin perintöjen aiheuttamilta tappioilta sekä identiteettivarkauksilta. Bitcoinissa kauppiaiden on mahdotonta pakottaa ei-toivottuja tai huomaamattomia maksuja. Läpinäkyvyydellä tarkoitetaan sitä, että Bitcoinissa tapahtuvat transaktiot ovat kaikkien nähtävillä lohkoketjuissa, eikä kukaan pysty niitä sieltä enää muokkaamaan (Bitcoin.org 2021).

Bitcoinilla on paljon potentiaalia, sillä Bitcoin on suunniteltu arvon säilyttäjäksi. Se on vielä tällä hetkellä kuitenkin liian pieni, sillä suuret tapahtumat, kaupat tai liiketoiminta vaikuttavat sen hintaan. Tämän uskotaan katoavan kunhan Bitcoin saa enenmmän käyttäjiä ja se alkaa hyötyä verkkoefektistä, jolloin sen hinnan vaihtelut katoavat (Bitcoin.org 2021).

4 Ethereum

Ethereum oli ensimmäinen ja nykypäivän suurin ohjelmoitavuutta varten optimoitu lohkoketju. Ethereum on krypto-ominaisuuksien (crypto asset) mukaan suunniteltu tukemaan täydellistä mukautettavuutta ja monimutkaisuutta. Tällä tarkoitetaan, että Ethereumilla voisi korvata kaikenlaisia finanssialan ongelmia ohjelmakoodilla, esimerkiksi stablecoinseilla, joista kuuluisimpia ovat Teather ja USDC. Ethereumin digitaalisten sopimusten avulla on luotu Compound, joka tuo lainaamisen lainanantajan ja lainanottajan välille ilman kolmansia osapuolia (Hougan 2020a).

4.1 Syntyperä

Ethereumin perustaja Vitalik Buterin sai ajatuksen Ethereumin kehittämisestä kehittäessään Bitcoinia. Hän tutustui lohkoketjuteknologiaan 17-vuotiaana vuonna 2011. Hän alkoi haaveilemaan alustasta, mikä antaisi enemmän käyttötapauksia kuin Bitcoinin taloudelliset mahdollisuudet. Vuonna 2013 hän julkaisi raportin kuvaamaan tätä ohjelmaa, joka johti Ethereumin syntyyn. Vuonna 2014 Buterin ja muut Ethereumin perustajat käynnistivät joukkorahoituskamppanjan. He myivät Ethereumin rahakkeita, Etheria, saadakseen näkemyksen sen kiinnostavuudesta. Joukkorahoituskamppanja tuotti yli 18 miljoonaa dollaria. Vuonna 2015 ensimmäinen Ethereum-livejulkaisu lanseerattiin, tämä kantoi nimeä Frontier (Marr 2018) (Hougan 2020b).

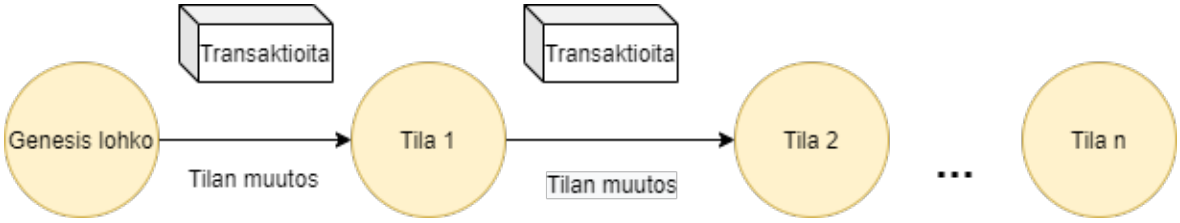
Ethereumin vakavin kriisi oli The Dao -projekti. Hyökkääjä pääsi käyttämään projektin koodissa ollutta haavoittuvuutta ja sai kerättyä yhteensä 3.6 miljoonaa Etheria. (Siegel 2016) Tapahtuma herätti paljon keskustelua jälkihoitonsa ansiosta. Osa oli sitä mieltä, että hakkeroinnin aiheuttamat tappiot pitäisi mitätöidä muokkaamalla Ethereumin lohkoketjua ja poistamalla Dao-hyökkäyksen aiheuttama vahinko. (Hyppänen 2020b) Ethereum-yhteisö äänesti siitä, tulisiko heidän tehdä hard fork Dao:n vahingon poistamiseksi. Kaikki Etherin omistajat pystyivät äänestämään transaktiolla carbonvote-nettisivulla. Hard forkin puolesta äänesti 85 prosenttia, joten hard fork tapahtui lohkon numero 192000 kohdalla ja Ethereum-lohkoketju jakautui kahtia (carbonvote.com 2016) (Buterin 2016). Nykyinen Ethereum on muokattu Et-

hereum, jossa hakkeroinnin aiheuttamat tappiot kumottiin muokkaamalla lohkoketjua. Ethereum Classic jatkaa vanhan lohkoketjun käyttöä. (Hyppänen 2020b)

Kryptovaluutat, joilla ei ole omaa erillistä lohkoketjuaan, mutta jotka käyttävät toisen salausresurssin lohkoketjua, tunnetaan tokeneina eli rahakkeina. Ethereum-verkossa olevia rahakkeita kutsutaan ERC-20-tokeneiksi. Kaikkien aikojen ensimmäinen ERC-tunnus, Augurniminen kryptovaluutta, käynnistettiin vuonna 2015. Siitä lähtien Ethereumin lohkoketjuun on luotu lukuisia tokeneita. Tällä hetkellä on yli 200 000 ERC-tunnusta, mikä tarkoittaa valtavaa kryptovaluuttaekosysteemiä yhden lohkoketjun varassa (ledger.com 2019).

4.2 Lohkoketjun toiminta

Ethereum-lohkoketju on pääasiallisesti transaktiohin perustuva tilakone. Ethereum-lohkoketju alkaa alkutilasta. Transaktion jälkeen alkutila vaihtuu uuteen tilaan niiden muodostumisen jälkeen, jolloin Ethereumin nykyinen tila on uusimmassa lohkossa (Kasireddy 2017). Alla oleva kuva hahmottaa kuinka Ethereum-lohkoketjun tila muuttuu transaktioiden myötä.



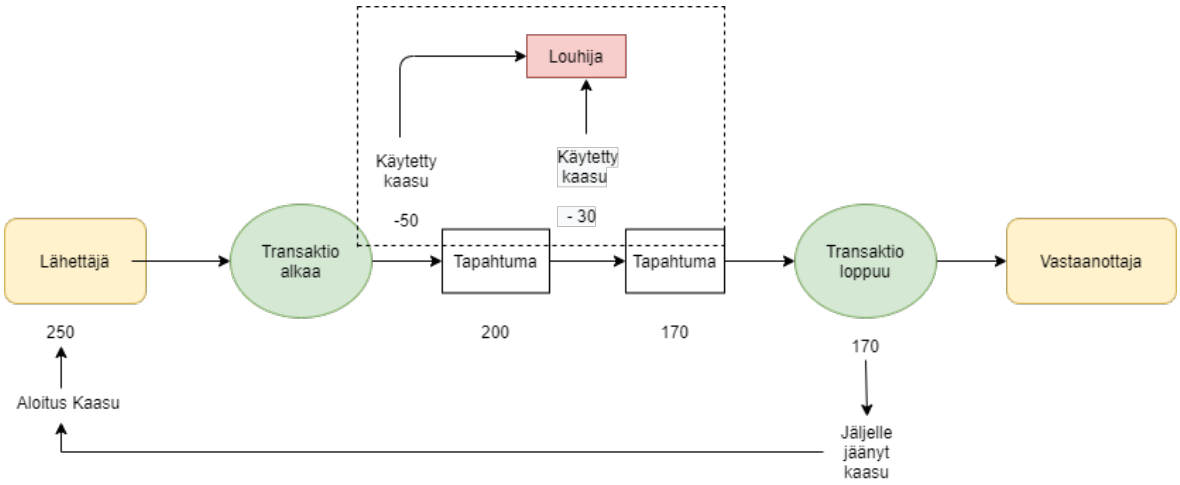
Kuvio 4. Kaavio Ethereumin tilan toiminnasta (Kasireddy 2017) esittämällä tavalla

Ethereum käyttää GHOST-protokollaa (Greedy Heaviest Observed Subtree) havaitsemaan, mikä polku on pätevin ja estää useiden ketjujen syntymisen. GHOST-protokollan mukaan paras polku on se, jolla on tehty eniten laskutoimituksia. Yksi tapa määrittää oikea polku on käyttää viimeistä lohkoa (lehtilohkoa), mikä edustaa lohkojen kokonaismäärää polulla. Mitä isompi lohkon numero on, sitä pidempi lohkoketju on ja tällöin sillä on suurempi louhintaan käytettävä työmäärä (Kasireddy 2017).

Ethereum koostuu useista pienistä tileistä. Jokaiselle tilille on liitetty tila ja 20:n tavun osoite. Tilejä on olemassa kahdenlaisia: ulkoisia omistustilejä ja sopimustilejä. Ulkoisia omistustilejä hallitaan yksityisillä avaimilla ja niihin ei ole liitetty koodia. Sopimustileihin on

liitetty koodeja ja niitä valvotaan omilla sopimuskoodeilla. Omistustileillä voi lähettää viestejä toiselle omistustilille tai sopimustileille luomalla ja allekirjoittamalla tapahtuman omalla yksityisellä avaimellaan. Kahden omistustilin välinen viesti on arvonsiirto, mutta viesti omistustililtä sopimustilille aktivoi sopimustilin koodin. Koodi voi pitää sisällään erilaisia toimintoja kuten tunnusten siirtämistä, laskutoimitusten suorittamista tai uuden sopimuksen luontia. Tilin tila koostuu neljästä osasta riippumatta tilin tyypistä. Nämä neljä ovat nonce, saldo, storageRoot ja codeHash (Kasireddy 2017).

Ethereumissa jokaisen Ethereum-verkon tapahtuman seurauksena tapahtumalaskelma perii maksun. Tätä maksua kutsutaan kaasuksi. Kaasu (gas) on yksikkö, jota käytetään laskennasta tulevien palkkioiden mittaamiseen. Kaasun hinta on se Etherin määrä, minkä lähettäjä on valmis käyttämään kyseisen tapahtuman suorittamiseksi. Jokaisessa tapahtumassa lähettäjä asettaa kaasurajan ja kaasun hinnan. Kaasuraja on suurin kaasun määrä, mitä käyttäjä on valmis käyttämään tapahtuman suorittamiseksi. Lähettäjä saa takaisin käyttämättömät kaasut kaupan lopussa ja ne vaihdetaan takaisin alkuperäisellä kurssilla. Jos kaasu loppuukin kesken tapahtuman ja se todetaan virheelliseksi, tapahtuman käsittely keskeytyy ja tilanne palautuu tilaan ennen tapahtumaa. Kuitenkin jos kone käytti jo vaivaa laskemisen suorittamiseen ennen kuin polttoaine loppui, niin tähän käytetty kaasu ei palaudu lähettäjälle. Lähettäjän lähettämät kaasut menevät suoraan louhijan osoitteeseen, sillä louhijat käyttävät työtehoa laskelmien suorittamiseksi ja liiketoimien validoimiseksi. Louhijoilla on valta valita mitä tapahtumia ne suorittavat, joten tämä saa aikaan sen, että suuremmalla kaasulla varustetut tapahtumat kiinnostavat enemmän louhijoita kuin pienet. He voivat myös ilmoittaa lähettäjille, millä vähimmäishinnalla ne suorittavat tapahtuman (Kasireddy 2017) (Bouraga 2020).



Kuvio 5. ETH transaktio kuvattu (Kasireddy 2017) mukaisesti

Ethereum-verkossa palkkioilla on oma tarkoituksensa. Ethereum on Turingin kone, joka voi simuloida mitä tahansa tietokonealgoritmia. Tämä mahdollistaa silmukat ja tekee Ethereumista alttiin pysähtymisongelmalle, jossa ei voida sanoa toimiiko ohjelma loputtomasti. Jos maksuja ei olisi, pahaa haluava taho voisi yrittää häiritä verkkoa suorittamalla loputtoman silmukan transaktiossa ilman seurauksia. Kaasumaksu suojaa verkkoa hyökkäyksiltä, sillä loputtoman silmukan pyörittäminen loppuu siinä kohtaa, kun kaasu loppuu lähettäjältä. Kaasumaksuja peritään myös tallennustilan käytön vuoksi. Tämän tarkoituksena on pitää Ethereum-tilatietokannan koko pienenä kaikissa solmuissa. Jokainen tallennustilan kasvu näkyy jokaisessa solmussa ja Ethereumin jokainen verkon suorittama yksittäinen operaatio suoritetaan samanaikaisesti jokaisen täyden solmun avulla (Kasireddy 2017) (Bouraga 2020).

Ethereumissa lohko koostuu lohkon otsikosta, tiedoista kyseiseen lohkoon sisältyvistä tapahtumaryhmistä ja Ommereiden lohko-otsikoista. Ommer on lohko, jonka vanhempi lohko on yhtä suuri kuin nykyisen lohkon vanhemman vanhempi. Ethereum on rakennettu niin, että lohkon aika on noin 13 sekuntia. Tämä mahdollistaa nopeammat transaktiot, mutta haittapuolena on se, että kaivostyöläiset löytävät enemmän kilpailevia lohkoratkaisuja. Näitä lohkoja kutsutaan myös orpolohkoiksi, koska lohkot on kaivettu, mutta ne eivät pääse pääketjuun. Ommerin tarkoitus on auttaa palkitsemaan louhijoita orpojen lohkojen säilyttämisestä. Ommer, jota louhija säilyttää, täytyy olla kelvollinen, eli sen on oltava nykyisen lohkon kuuden-

nessa tai sitä pienemmässä sukupolvessa. Kuudennen sukupolven jälkeen orpoihin lohkoihin ei voida enää viitata. Ommer-lohkoista saa pienemmän palkkion kuin täydestä lohkosta. Kuitenkin louhijoiden on silti kannattavaa säilyttää orpolohkot ja saada siitä palkkio (Kasireddy 2017).

4.3 Ominaisuudet

Ethereum-ekosysteemi mahdollistaa erilaiset sopimukset eri järjestelmissä. Tällaisia voisivat olla esimerkiksi valuutanvaihto ja osakkeet. Ethereumin lohkoketjun mahdollisuudet eivät kuitenkaan rajoitu pelkästään tähän, vaan hyviä mahdollisuuksia ovat myös äänestäminen, resurssien hallinta ja erilaiset älysopimukset. (Hyppänen 2020b). Älysopimuksilla tarkoitetaan lohkoketjuun tallennettavaa ohjelmakoodia, joka tulee tapahtumaan varmasti, kun ehdot täyttyvät. (Chen ym. 2018)

Ethereumilla on samoja ominaisuuksia kuin Bitcoinilla. Ethereum on täysin digitaalinen kryptovaluutta Ether (ETH), jota voidaan lähettää kenelle vaan ympäri maailmaa. Myöskään ETH tarjonnan määrää ei ohjaa mikään yksittäinen taho, vaan se on sidottu tiettyyn määrään. Ethereum-lohkoketju pystyy paljon muuhunkin kuin tavalliset lohkoketjut, sillä Ethereum on ohjelmoitavissa. Tämä tarkoittaa sitä, että sen kehittäjät voivat rakentaa sillä uudenlaisia sovelluksia. Näitä sovelluksia kutsutaan desentralisoiduiksi sovelluksiksi (decentralized applications, dapps) (Ethereum.org 2021c) (Chen ym. 2018). Ethereumin luojan Vitalik Buterin ajatuksena oli luoda samanlainen toimintaympäristö kuin esimerkiksi mobiilisovelluksilla on. Tällä hetkellä mobiilisovelluksien tekijät voivat laittaa Google Play -sovelluskauppaan valmiit sovelluksensa ihmisten ladattavaksi. Sovelluskehittäjillä on siis mahdollisuus luoda sovelluksia tiettyjen ohjelmointirajapintojen ja työkalujen mukaisesti, jolloin kaikki sovellukset on tehty yhteisten sääntöjen mukaisesti (Hyppanen 2021). Sovellusten etu on siinä, että Ethereum-lohkoketjussa ne ajetaan aina niin kuin ne on ohjelmoitukin ja ne on hajautettu Ethereumin mukana. (Ethereum.org 2021c)

5 Arvon määräytyminen

Kryptovaluuttojen hinta määräytyy Bitcoinin tapaan kysynnän ja tarjonnan perusteella. Kun Bitcoinien kysyntä kasvaa, hinta nousee, ja kysynnän laskiessa hinta laskee. Liikkeessä on vain rajoitettu määrä Bitcoineja ja uusia Bitcoineja luodaan ennustettavalla ja laskevalla nopeudella, mikä tarkoittaa, että kysynnän on noudatettava tätä inflaatiotasoa, jotta hinta pysyy vakaana. Koska Bitcoin on edelleen suhteellisen pieni markkina verrattuna siihen, mitä se voisi olla, se ei vaadi merkittäviä määriä rahaa markkinahinnan siirtämiseksi ylös tai alas, ja siten Bitcoinin hinta on edelleen hyvin epävakaa (bitcoin.org 2021). Tämän takia Bitcoin-markkinat ovat hyvin alttiina hintakuplille. (A. S. Hayes 2018)

Minkä takia ihmiset antavat kryptovaluutoille arvoa? Valuutalla on arvoa, jos sitä voi käyttää luotettavasti arvovarastona eli se pystyy pitämään arvoa yllä ajan mittaan. Bitcoinin tapauksessa tähän vaikuttaa kuusi tekijää: niukkuus, jaettavuus, apuohjelmat, kuljetettavuus, kestävyys ja väärentäminen. Niukkuudella tarkoitetaan sitä, että Bitcoinia on olemassa vain 21 miljoonaa. Sitä ei voi painaa lisää kuten tavallista rahaa. Jaettavuudella tarkoitetaan, että Bitcoinia voi jakaa paljon pienempiin osiin. Pienin Bitcoinin osa on satoshi, joka on 0,00000001 Bitcoinia. Apuohjelmilla tarkoitetaan lohkoketjuteknologiaa. Sen avulla Bitcoinin kirjanpitojärjestelmä on hajautettu ja luotettava. Kuljetettavuudella tarkoitetaan valuutan siirtoa puolelta toiselle. Bitcoin on siirrettävissä muutamassa minuutissa hyvin pienillä kustannuksilla. Kestävyydellä tarkoitetaan sitä, että se ei ole tuhottavissa samalla tavalla kuin normaali seteliraha. Väärennöksillä puolestaan tarkoitetaan, että Bitcoinia ei voi väärentää lohkoketjuteknologian ansiosta. Ainoastaan kaksinkertaisella kulutuksella on teoriassa mahdollista saada väärennös onnistumaan, mutta tähän tarvittaisiin todella paljon resursseja (Kelleher 2021).

Meneistyneimmät kryptovaluutat yrittävät ratkaista reaalimaailman ongelmia. Tutkielmassa esille tullut Bitcoin yrittää ratkaista fiat-rahalla olevia ongelmia, kun taas Ethereum pyrkii ratkaisemaan liikemaailman sopimusongelmia. Jos kryptovaluutta ei saa ihmisten kiinnostusta sen arvo jää hyvin äkkiä matalalle tasolle (Northcrypto.com 2018).

6 Mitä eroja Bitcoinilla ja Ethereumilla on?

Bitcoinilla ja Ethereumilla on paljon samoja ominaisuuksia kuten lohkoketjun käyttäminen, hajautus ja läpinäkyvyys transaktioissa. Ne ovat kuitenkin täysin erilaisia valuuttoja, kun vertaillaan niiden suunnittelua ja käyttökohdetta. Bitcoinin pääkäyttökohde on maksuvaluutta, kun taas Ethereum-lohkoketju on suunniteltu mahdollistamaan paljon enemmän businessmaailman käyttökohteita. Ethereumin etuna on se, että se pystyy toteuttamaan älykkäitä sopimuksia, mikä ovat herättänyt kiinnostuksen yrityksissä (Milutinović 2018).

Ethereumin lohkojen välinen aika on lyhyempi kuin Bitcoinin. Ethereum-lohkojen välissä on noin 13 sekuntia, kun taas Bitcoinissa tämä sama aika on noin 10 minuuttia. (BitInfoCharts 2021)(ycharts.com 2021) Tämä tarkoittaa, että Bitcoinin transaktio kestää 10 minuuttia, sillä Bitcoin luo lohkon noin 10 minuutin välein. Ethereum luo lohkon 13 sekunnin välein. (Antonylewis2015 2016)

Ethereum-lohkoketjun koko on pienempi kuin Bitcoinin. Bitcoin-lohkon maksimikoko määritetään tavuissa, mikä tällä hetkellä on 1.3 MB. (blockchain.com 2021) Ethereumin lohkokoko perustuu suoritettavien sopimusten monimutkaisuuteen. Tämä tunnetaan termillä kaasuraja lohkoa kohden ja maksimimäärä voi vaihdella lohkosta toiseen. Tällä hetkellä Ethereumin lohkokoko on noin 1,5 miljoonaa kaasua. Perustapahtuman tai tililtä toiselle tapahtuvan ETH-maksun monimutkaisuus on 21 tuhatta kaasua, joten keskimäärin lohkoon mahtuu noin 70 transaktiota (Antonylewis2015 2016). Etherscan (2021) saadun datan mukaan Ethereum-lohkojen koko lähentelee 50 000 tavua, joka megatavuissa on noin 0.05.

Ethereumilla Virtual Machine hoitaa älysopimuksien koodeja. (Chen ym. 2018) Nämä toimivat kaikkien verkkoon osallistuvien tietokoneilla. Monesti Ethereumin älykkäitä sopimuksia kutsutaan nimellä Turing Complete, millä tarkoitetaan, että sopimukset ovat täysin toimivia ja ne voi suorittaa millä tahansa ohjelmointikielellä (Antonylewis2015 2016). Bitcoin-verkko ei pysty suorittamaan ollenkaan älysopimuksia.

Ethereumilla ja Bitcoinilla on eroja myös tokeneiden luomisen suhteen. Bitcoinilla tokeneiden eli rahakkeiden maksimimäärä on teoriassa 21 miljoonaa ja uusien luomisnopeus puolittuu neljän vuoden välein. Ethereumissa taas jatketaan Etherin tuotantoa vakiomäärällä vuo-

dessa. Etherin olemassa oleva määrä tulee neljän eri palkkion yhteenlaskuna. Nämä ovat esikaivos, lohkopalkkio, Ommer-palkkiot ja Ommer:n viittaava palkkio. Esikaivoksessa luotiin 72 miljoonaa Etheriä, jotka myytiin rahoitusmyynnissä heinä-elokuussa 2014. Tämän jälkeen päätettiin, että ETH-sukupolven koko saa kasvaa 25 prosenttia vuodessa esikaivoksen myynnin määrästä, joka on siis 18 miljoonaa. Etheriä louhitaan enintään vuosittain 18 miljoonaa. Jokainen louhittu lohko luo 5 ETH:tä per lohko. Uusi lohko löytyy noin 13 sekunnin välein, jolloin vuodessa ETH:tä syntyy 11,3 miljoonaa (Antonylewis2015 2016).

Ethereumin kuten Bitcoininkin lohkojen louhinnassa syntyy niin sanottuja orpolohkoja, jotka on louhittu myöhässä, niin etteivät ne ole osa päälohkoketjua. Bitcoinissa nämä lohkot hylätään. Ethereumissa nämä orvot otetaan mukaan ja niitä kutsutaan Ommer-lohkoiksi (Ethereum.org 2021a). Jokaisesta louhitusta Ommer-lohkosta louhija saa palkinnoksi 7/8 osaa täydestä lohkopalkkiosta. Tämä tuo 0.7 miljoonaa ETH lisää palkkiota vuodessa. Ommer-lohkoihin voi myös viitata. Louhija voi viitata setä-lohkoon ja saa tästä 0.15 ETH per Ommer-lohko. Louhija ei voi kuitenkaan viitata kuin kahteen Ommer-lohkoon kerrallaan (Antonylewis2015 2016).

Chen ym. (2018) tutkimuksessaan toteavat Ethereumilla ja Bitcoinilla on eroa rahakkeiden siirtymisessä. Aiemmin alaluvussa 4.2 Lohkoketjun toiminta kerrotaan Ethereumilla olevan kahdenlaisia tilejä, joiden välillä transaktiot ja sopimukset tapahtuvat. Ethereumissa tili sisältää tiedon rahatilanteesta, mutta Bitcoinissa ei tälläistä ominaisuutta ole. Bitcoinilla ei ole ollenkaan edes tilejä vaan käyttäjän bitcoinlompakko laskee tiedon itse lohkoketjusta.

7 Yhteenveto

Bitcoin on tuttu kryptovaluutta lähes kaikille ihmisille. Se on ollut olemassa jo yli 10 vuotta. Tämä onkin Bitcoinin suurin etu nuorten kryptovaluuttojen rinnalla. Kryptovaluuttojen arvo perustuu kysyntään, jolloin tunnetuinta kryptovaluuttaa ostetaan todennäköisimmin. Bitcoinien rajallinen määrä tuo myös mahdollisesti etua kilpailijoihinsa nähden. On kuitenkin vaikea sanoa mitä Bitcoinin arvolle tapahtuu sitten, kun Bitcoinin murusetkin on louhittu. Oma ajatukseni on, että Bitcoinin arvo voi lähteä liikkumaan arvaamattomasti jos kysyntä pysyy samanlaisena, sillä luvussa 5 mainittu inflaatiotaso ei ole enää tasaamassa Bitcoinin hintaa.

Bitcoinin tulevaisuudesta löytyy paljon kehitettäviä asioita pohdittavaksi. Uusien Bitcoinien syntyminen tulee loppumaan vääjäämättä tulevaisuudessa. Noin vuonna 2140 viimeinenkin Bitcoin on louhittu. Tämä tulee vaikuttamaan ainakin Bitcoinin louhintaan ja sitä kautta mahdollisesti arvoonkin, sillä tällä hetkellä uuden lohkon löytämisestä tulevat lohkopalkkiot kannustavat louhijoita jatkamaan louhintaa. Kun lohkopalkkioita ei enää tule, täytyy louhinnasta tehdä toisella tavalla kannattavaa. Tähän vaihtoehtona olisi transaktiomaksun nostaminen (A. Hayes 2021). Toinen Bitcoinin tulevaisuuden ongelma on sen käyttämä PoW-konsensusalgoritmi. Sitä suorittavat tietokoneet kuluttavat paljon sähköä, eikä täten ole tulevaisuutta ajatellen kovinkaan käytännöllinen. Tästä syntyikin toukokuussa 2021 suurehko Bitcoin kriisi kun Elon Musk twiittasi Twitterissä Teslan lopettavan autojensa myymisen Bitcoineilla, Bitcoinin louhinnan ympäristövaikutuksiin vedoten.

Ethereumin tilanne vaikuttaa olevan valoisampi Bitcoinilla esiintyvien ongelmien suhteen. Aiemmin edellisessä luvussa todettiin Etheria syntyvän joka vuosi vakio määrä, joten louhinnan loppumisen ei pitäisi aiheuttaa epävakautta. Ethereum on myös siirtymässä PoW -louhinnasta PoS -louhintaan Ethereum 2.0 päivityksen avulla. Tämä on kuitenkin vielä täysin alkutekijöissään oleva projekti, joten eteen tulee varmasti vielä monta ongelmaa.

Mitkä sitten ovat Ethereumin edut? Ethereumin suurimpia valtteja ovat älysopimukset sekä sen ekosysteemi. Älysopimuksien ansiosta Ethereum on monipuolisempi transaktioiden osalta kuin Bitcoin. Lisäksi Ethereum-ekosysteemi tarjoaa muille mahdollisuuden rakentaa omia kryptovaluuttojaan tai sovelluksia Ethereum-lohkoketjuun, mikä ei ole Bitcoinissa

mahdollista. Ethereum-lohkoja syntyy myös nopeammin ja lohkoketjun rakentumisessa syntyneitä orpoja lohkoja otetaan hyötykäyttöön.

Oma näkemykseni on, että vaikka Ethereumin lohkoketjussa on enemmän ominaisuuksia kuin Bitcoinilla, ne kilpailevat eri sarjoissa. Bitcoinin tarkoituksena on olla arvon säilyttäjä, kun taas Ethereum on ekosysteeminä muille. Molemmilla on kuitenkin omat rahakkeensa, joista Bitcoin on tällä hetkellä arvokkaampi. Uskon, että tulevaisuudessa Ethereumin Etherillä on mahdollisuudet päästä Bitcoinin tasolle, jos se saa riittävästi kannattajia.

Tämä katsaus on vain pintaraapaisu kryptovaaluuttojen maailmaan. Molemmat esitetyt kryptovaluutat ovat vielä kehitysvaiheessa ja saavat varmasti tulevaisuudessa paljon uusia päivityksiä, joista suurin on näillä näkymin Ethereum 2.0. Kryptovaluutat ovat hyvin nuori aihealue, joten tutkittavaa on vielä paljon. Tutkimustietoa löytyy mielestäni aika rajallisesti eikä esimerkiksi arvioita Bitcoinin tulevaisuudesta louhintapalkkion loputtua ollut helposti löydettävissä. Seuraavia tutkimuskohteita voisivat olla kolmannen sukupolven kryptovaluuttojen tuominen vertailuun mukaan, uutisissa jo esillä olleet kryptovaluuttojen ympäristövaikutukset tai aiemmin tässä kappaleessa pohdittu Bitcoinin tulevaisuus.

Lähteet

Acharjamayum, Irani, Ripon Patgiri ja Dhruwajita Devi. 2018. “Blockchain: A Tale of Peer to Peer Security”. Teoksessa *2018 IEEE Symposium Series on Computational Intelligence (SSCI),* 609–617. https://doi.org/10.1109/SSCI.2018.8628826.

Antonylewis2015. 2016. *A gentle introduction to Ethereum.* Https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/ Luettu: 14.2.2021.

Best, Raynor de. 2021. *Number of cryptocurrencies worldwide from 2013 to 2021.* Https://www.statista.c crypto-coins-tokens/.

Bitcoin.org. 2021. *What are the advantages of Bitcoin?* Https://bitcoin.org/en/faqwhat-are-the-advantages-of-bitcoin.

bitcoin.org. 2021. *What determines bitcoin‘s price?* Https://bitcoin.org/en/faqwhat-determines-bitcoins-price.

BitInfoCharts. 2021. *Bitcoin Block Time historical chart.* Https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html.

blockchain.com. 2021. *Average Block Size (MB).* Https://www.blockchain.com/charts/avg-block-size.

Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll ja Edward W. Felten. 2015. “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”. Teoksessa *2015 IEEE Symposium on Security and Privacy,* 104–121. https://doi.org/10.1109/SP.2015.14.

Bouraga, Sarah. 2020. “An Evaluation of Gas Consumption Prediction on Ethereum based on Transaction History Summarization”. Teoksessa *2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS),* 49–50. https://doi.org/10.1109/BRAINS49436.2020.9223288.

Buterin, Vitalik. 2016. *Hard Fork Completed.* Https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

carbonvote.com. 2016. *Vote: TheDAO Hard Fork.* Http://v1.carbonvote.com/.

Chen, Ting, Yuxiao Zhu, Zihao Li, Jiachi Chen, Xiaoqi Li, Xiapu Luo, Xiaodong Lin ja Xiaosong Zhange. 2018. "Understanding Ethereum via Graph Analysis". Teoksessa *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications,* 1484–1492. https://doi.org/10.1109/INFOCOM.2018.8486401.

cmcmarkets.com. 2021. *What are cryptocurrencies?* Https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-are-cryptocurrencies.

CoinMarketCap. 2021. *Today's Cryptocurrency Prices by Market Cap.* Https://coinmarketcap.com/ Luettu: 14.5.2021.

Ethereum.org. 2021a. *Glossary.* Https://ethereum.org/en/glossary/ommer.

———. 2021b. *Popular types of token.* Https://ethereum.org/en/eth/.

———. 2021c. *WHAT IS ETHEREUM?* Https://ethereum.org/en/what-is-ethereum/.

Etherscan. 2021. *Ethereum Average Block Size Chart.* Https://etherscan.io/chart/blocksize.

Finansivalvonta. 2019. *Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu.* Https://www.finanssivalvonta.fi/kuluttajansuoja/kysymyksia-ja-vastauksia/virtuaalival

Floyd, David. 2020. *How Bitcoin Works.* Https://www.investopedia.com/news/how-bitcoin-works/ Luettu:14.5.2021.

Frankenfield, Jake. 2019. *Proof of Stake (PoS).* Https://www.investopedia.com/terms/p/proof-stake-pos.asp.

Hayes, Adam. 2021. *What Happens to Bitcoin After All 21 Million Are Mined?* Https://www.investopedia happens-bitcoin-after-21-million-mined/.

Hayes, Adam S. 2018. *Bitcoin price and its marginal cost of production: support for a fundamental value.* Https://www-tandfonline-com.ezproxy.jyu.fi/doi/full/10.1080/13504851.2018.1488040.

Hou, Binbing, ja Feng Chen. 2020. "A Study on Nine Years of Bitcoin Transactions: Understanding Real-world Behaviors of Bitcoin Miners and Users". Teoksessa *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS),* 1031–1043. https://doi.org/10.1109/ICDCS47774.2020.00091.

Hougan, Matt. 2020a. *Why Ethereum Has Value - The Opportunity In Programmable Money 'DeFi'*. Https://www.forbes.com/sites/matthougan/2020/07/13/why-ethereum-has-valuethe–opportunity-in-programmable-money–defi/?sh=6f0ee88c4818.

———. 2020b. *Why Ethereum Has Value - The Opportunity In Programmable Money 'DeFi'*. Https://ethereum.org/en/history/.

Hyppanen, Antti. 2021. *Ethereum on platformien kuningas.* Https://bitcoinkeskus.com/ethereum-opas/.

Hyppänen, Antti. 2020a. *Opas: Bitcoin Cash.* Https://bitcoinkeskus.com/bitcoin-cash/.

———. 2020b. *Opas: Ethereum.* Https://bitcoinkeskus.com/ethereum-opas/.

Iredale, Gwyneth. 2020. *6 Key Blockchaun Features You Need to Know Now*. Https://101blockchains.com to-blockchain-features.

Johansson, Patrik Elias, Mikko Eerola, Antti Innanen ja Juha Viitala. 2019a. "Lohkoketju Tiekartta Päättäjille". Luku 1.0.2, 27–29. Alma Talent Oy.

———. 2019b. "Lohkoketju Tiekartta Päättäjille". Luku 1.1.1, 58–60. Alma Talent Oy.

———. 2019c. "Lohkoketju Tiekartta Päättäjille". Luku 1.1.1, 56–57. Alma Talent Oy.

———. 2019d. "Lohkoketju Tiekartta Päättäjille". Luku 1.1.1, 62–63. Alma Talent Oy.

———. 2019e. "Lohkoketju Tiekartta Päättäjille". Luku 1.0.2, 29–30. Alma Talent Oy.

———. 2019f. "Lohkoketju Tiekartta Päättäjille". Luku 1.2.1, 97–98. Alma Talent Oy.

———. 2019g. "Lohkoketju Tiekartta Päättäjille". Luku 1.2.1, 30–31. Alma Talent Oy.

Kasireddy, Preethi. 2017. *How does Ethereum work, anyway?* Https://preethikasireddy.medium.com/how does-ethereum-work-anyway-22d1df506369 Luettu: 14.2.2021.

Kelleher, John P. 2021. *Why do bitcoins have value?* Https://www.investopedia.com/ask/answers/100314/ do-bitcoins-have-value.asp.

Kryptovaluutta.fi. 2021. *Bitcoin louhinta.* Https://www.kryptovaluutta.fi/bitcoin-louhinta.

ledger.com. 2019. *A brief history on Bitcoin Cryptocurrencies.* Https://www.ledger.com/academy/crypto/brief-history-on-bitcoin-cryptocurrencies.

Marr, Bernard. 2018. *Blockchain: A Very Short History Of Ethereum Everyone Should Read.* Https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/?sh=451315131e89.

Milutinović, Monia. 2018. "Cryptocurrency". *Ekonomika* 64 (tammikuu): 105–122. https://doi.org/10.5937/ekonomika1801105M.

Mooter, David. 2020. *he Bitcoin Blockchain Explained.* Https://medium.com/swlh/the-bitcoin-blockchain-explained-b4529c78e6af Luettu: 13.5.2021.

Nair, P. Rajitha, ja D. Ramya Dorai. 2021. "Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain". Teoksessa *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV),* 279–283. https://doi.org/10.1109/ICICV50876.2021.9388487.

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Https://bitcoin.org/bitcoin.pdf

Northcrypto. 2018. *Mikä on lohkoketju?* Https://www.northcrypto.com/fi/about/blockchain.

Northcrypto.com. 2018. *Mitä ovat kryptovaluutat?* Https://www.northcrypto.com/fi/about/cryptocurrency

Peters, Katelyn. 2021. *A History of Bitcoin Hard Forks.* Https://www.investopedia.com/tech/history-bitcoin-hard-forks/.

Reiff, Nathan. 2020. *Blockchain Technology's Three Generations.* Https://www.investopedia.com/tech/bl technologys-three-generations/.

Royal, James, ja Kevin Voigt. 2021. *What Is Cryptocurrency? Here's What You Should Know.* Https://www.nerdwallet.com/article/investing/cryptocurrency-7-things-to-know.

Siegel, David. 2016. *Understanding The DAO Attack.* Https://www.coindesk.com/understanding-dao-hack-journalists.

ycharts.com. 2021. *Ethereum Average Block Time.* Https://ycharts.com/indicators/ethereum$_a$*verage*$_b$*lock*