LOHKOKETJUJEN HYÖDYNTÄMINEN

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Hämeenlinna

syksy 2017

Mika Himanen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn tradenomi
Hämeenlinna

Tekijä Mika Himanen **Vuosi** 2017

Työn nimi Lohkoketjujen hyödyntäminen

Työn ohjaaja/t Erkki Laine

TIIVISTELMÄ

Opinnäytetyöni tavoite oli selventää mistä lohkoketjuissa on kyse: mitä lohkoketjut varsinaisesti ovat ja mihin niitä käytetään. Työssä annetaan läpileikkaus lohkoketjututkimuksen tämänhetkiseen tilaan ja arvioita tulevaisuuden kehityksestä lohkoketjujen ympärillä.

Työssä esitellään lyhyesti useita lohkoketjuihin liittyviä hankkeita ja tutkimuskohteita. Painopisteenä on esitellä mahdollisimman erilaisia hankkeita niin yksityiseltä kuin julkiselta sektorilta.

Keskeisenä havaintona huomataan, että lohkoketjuja ja niiden ympärillä käytävää tutkimusta ja keskustelua leimaa epävarmuus. Varsinaisia vakiintuneita toteutuksia ei Bitcoinia lukuun ottamatta juurikaan vielä ole, mutta paljon käynnissä olevaa tutkimus- ja kehitystyötä tehdään runsaasti.

Asiantuntijoiden näkemyksen mukaan lohkoketjut lyövät itsensä läpi varsinaisesti vasta 5-10 vuoden kuluessa, mutta sitä ennen selvitettävänä on vielä monia teknisiä, lainsäädännöllisiä ja käytännöllisiä haasteita.

Avainsanat lohkoketjut, blockchain, Ethereum, bitcoin, virtuaalivaluutta

Sivut 27 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Hämeenlinna

Author Mika Himanen **Year** 2017

Subject Benefiting from blockchains

Supervisor Erkki Laine

ABSTRACT

The goal of this thesis is to clarify both what blockchains are about and how they are currently used. The thesis will provide a cross-section of the current state of blockchain research and estimates of the future development concerning blockchains.

The thesis provides a compact summary several blockchain-related projects and research ventures. The thesis focuses on outlining projects extensively from both public and private sectors.

The main observation is that blockchains, and the discussion and research surrounding them, are filled with uncertainties. Established applications beside Bitcoin are close to non-existent, but research and development is plentiful.

The expert opinion seems to be that the blockchain will break through in 5 to 10 years, but before that there are many technical, legal and practical challenges.

Keywords blockchain, Ethereum, bitcoin, virtual currencies

Pages 27 pages

SISÄLLYS

1 JOHDANTO

Opinnäytetyöni aiheeksi valitsin lohkoketjut ja niiden käytön. Lohkoketjut ovat ajankohtainen ja mielenkiintoinen aihe, josta suomenkielistä materiaalia löytyy toistaiseksi melko vähän. Lohkoketjuista puhutaan paljon, niitä sanotaan mullistavaksi keksinnöksi ja niiden käyttömahdollisuuksista annetaan optimistisia lausuntoja, mutta mikä osa on teknologiahypeä ja mikä valideja tulevaisuudenkuvia?

Opinnäytetyössäni pyrin ensinnäkin valaisemaan mitä lohkoketjut ovat: mitä teknologioita, tekniikoita ja käsitteitä niihin liittyy ja mikä on lohkoketjuteknologian varsinainen anti. Tämä edellyttää peruskäsitteistön selventämistä, jotta myös alaan perehtymättömät voivat saada käsityksen mistä lohkoketjuissa on kyse.

Tärkeänä lohkoketjujen turvallisuuteen liittyvänä asiana selvennän, mitä hajautusarvot ja hajautusfunktiot ovat ja miten niitä käytetään lohkoketjuissa. Esittelen louhinnan ja työn osoituksen käsitteet ja miten niitä lohkoketjuissa käytetään, tarkempana esimerkkinä perehtyen tunnetuimpaan ja suurimpaan lohkoketjutoteutukseen, Bitcoiniin.

Työssä esitellään joitain käynnissä olevia lohkoketjuhankkeita, keskittyen mahdollisimman laaja-alaisesti mielenkiintoisiin, ajankohtaisiin ja eri näkökulmista lohkoketjuja hyödyntäviin projekteihin.

Pyrin myös antamaan jonkinlaisen kuvan lohkoketjujen ympärillä tapahtuvasta tutkimuksesta ja lohkoketjujen käyttökohteista sekä antamaan viitteitä mihin niitä tullaan todennäköisesti käyttämään lähitulevaisuudessa.

2 LOHKOKETJUT

Lohkoketjut (alk. block chains, nyk. blockchains) ovat Satoshi Nakamoton Bitconia varten kehittämä teknologia (Nakamoto 2008, 1). Satoshi Nakamoto on pseudonyymi, jonka takana olevaa henkilöä tai henkilöitä ei tunneta. Tiiviisti ilmaistuna lohkoketjut ovat vertaisverkkoon hajautettuja tietokantoja, joitten luotettavuutta varmistetaan kryptografisin menetelmin.

Lohkoketjut koostuvat peräkkäisistä lohkoista, jotka sidotaan toisiinsa louhimalla uusia lohkoja ja sijoittamalla uusin louhittu lohko ketjun päätteeksi. Louhiminen tapahtuu suorittamalla jokin osoitus, kuten esimerkiksi työn osoitus tai osakkuuden osoitus ja lisäämällä osoituksen todistus louhittavaan lohkoon.

Lohkoketjujen toteuttaminen vaatii ratkaisuja mm. siihen, miten lohkon haarautumisristiriidat ratkaistaan ja millä protokollalla lohkoketjujen käyttäjät viestivät vertaisverkossa. Jokaisen lohkoketjutoteutuksen täytyy tehdä omat valintansa ratkaisujen suhteen. Bitcoinin toteutuksen valintoja käsitellään tarkemmin Bitcoinia käsittelevässä luvussa. Vaihtoehtoisia toteutuksia ja ratkaisuja käsitellään luvussa 4, Bitcoinin perilliset.

Lohkoketjut yhdistävät useita aiemmin käytössä olleita menetelmiä, tekniikoita ja konsepteja yhteen. Tärkeinä vaikuttimina ovat olleet mm. roskasähköpostin ehkäisyä varten luotu Hashcode (josta saatiin idea työn osoituksesta), vertaisverkot ja julkisiin avaimiin perustuvat salausjärjestelmät. (Franco 2015, 163–167.)

2.1 Lohkoketjuihin liittyviä termejä

Tietoverkkojen voidaan ajatella koostuvan solmuista (tietoverkossa kiinni olevista laitteista) ja niiden välisistä yhteyksistä. Vertaisverkot ovat tapa järjestää tietoverkon solmut toisiinsa. Vertaisverkossa kaikki solmut ovat tasaveroisia toistensa kanssa eivätkä hierarkkisesti, esimerkiksi palvelin–asiakas-suhteessa. Solmut ovat yleensä yhteydessä useaan toiseen solmuun. Vertaisverkkoja vastaan on hankala tehdä palvelunestohyökkäyksiä, sillä yksittäisen solmun kuormittaminen ei haittaa muuta verkkoa. (TSK n.d.)

Tunnetuimpia ja käytetyimpiä vertaisverkkosovelluksia ovat torrent-pohjaiset tiedostonsiirtojärjestelmät, mutta myös Windows 10 käyttää päivitystensä lataamiseen vertaisverkkoa jos käyttäjän asetukset tämän sallivat. Spotify käyttää myös vertaisverkkoa musiikin ja videoiden välittämiseen.

Tiedostojen lataaminen vertaisverkosta on tehokasta, koska tiedostot ovat jaettuina paloiksi ja jokainen vertaisverkon jäsen voi jakaa toisille jäsenille jo lataamiaan paloja. Näin tiedostonsiirtokapasiteetti kasvaa käyttäjien myötä.

Hajautettu tietokanta ei sijaitse keskitetysti millään yksittäisellä palvelimella, vaan tietokannan ja sen tietojen kopioita säilytetään hajautetusti eri puolilla verkkoa. Hajautettu tietokanta toteutetaan usein vertaisverkkona. (IATE n.d.)

Avoimen lähdekoodin järjestelmillä (open source) tarkoitetaan ohjelmistoja, joiden lähdekoodin kuka tahansa voi ladata, halutessaan muokata ja kääntää lähdekoodin suoritettavaksi ohjelmaksi joko sellaisenaan tai muokattuna. (TSK n.d.)

Avoimen lähdekoodin puolustajat sanovat sen lisäävän luotettavuutta, ja erityisesti virtuaalivaluutoissa avoin lähdekoodi mahdollistaa ryhmätarkkailun: esimerkiksi virtuaalivaluutan koodissa voidaan olla varmoja, että siinä ei ole piilotettuja ohjelmanpätkiä, jotka vaikkapa siirtäisivät valuuttaa valuuttaohjelmiston tekijälle käyttäjän tietämättä.

Luotettavuus on kaksijakoinen käsite. Sillä tarkoitetaan ensinnäkin luottamusta siihen, että lähettäjä on kuka väittää olevansa. Toisekseen sillä tarkoitetaan luottamusta siihen, että lähetetty tieto on välitetty muuttumattomana vastaanottajalle. (VM 2008.) Luotettavuusongelmien ratkaiseminen on kryptografian perusongelmia, ja siihen on tehty useita ratkaisuja.

Lohkoketjujen yhteydessä luotettavuus on yleensä ratkaistu julkisen avaimen salauksilla, jota internetissä käytetään yleisesti tietojen salaukseen, mm. salattujen internetyhteyksien luomisessa käytettävässä SSL-protokollassa.

Julkisen avaimen menetelmä (public key cryptography) perustuu avainpariin: julkiseen ja salaiseen avaimeen. Julkinen avain nimensä mukaisesti voidaan julkistaa missä tahansa, esim. sähköpostiviestin allekirjoituksessa tai verkkosivuilla. Salainen eli yksityinen avain on sen sijaan pidettävä aina hyvin suojattuna. (VM 2008.)

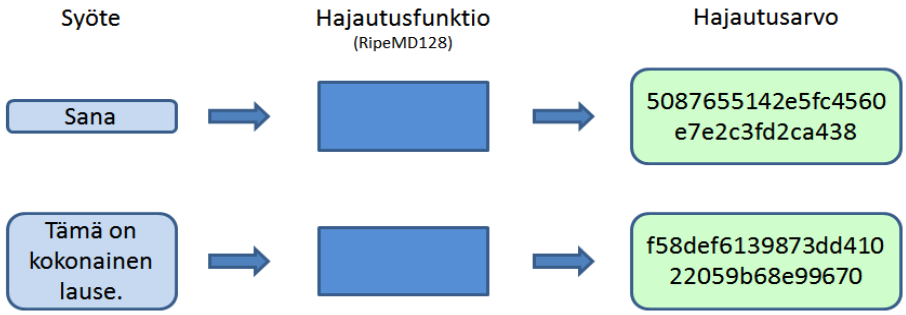
Esimerkiksi sähköpostiviestejä salatessa lähettäjä allekirjoittaa (eli kryptaa) viestin vastaanottajan julkisella avaimella jolloin viesti salataan. Salatun viestin voi purkaa ainoastaan vastaanottajan yksityisellä avaimella.

2.2 Hajautusarvot

Hajautusarvo (hash value) on tiedosta hajautusfunktiota (hash function) käyttäen muodostettu, usein lyhyempi uusi tieto varmisteen muodostamiseksi tai hajakoodauksessa käytettäväksi (VM 2008). Hajautusfunktio tuottaa eripituisista syötteistä aina samanpituisen tuloksen ja samanlaisista syötteistä hyvin erilaisia tuloksia. Näistä syistä se on yleisesti käytetty menetelmä kryptografiassa, sillä tuloksista on laskennallisesti vaikeaa selvittää alkuperäinen syöte. (IATE n.d.)

Hajautusarvoista ja hajautusfunktioista käytetään myös muotoja tiiviste ja tiivistysfunktio, mutta pääosin yhteyksissä joissa tiivistefunktioilla muodostetaan esim. tarkistussummia tiedostoista. (IATE n.d.)

Hajautusarvojen murtamisessa ainoa keino on ns. väsytyshyökkäys, jossa tietokone kokeilee kaikkia mahdollisia syötteitä kunnes vastaava hajautusarvo löytyy. Tämä on luonnollisestikin hyvin aikaa vievää ja laskennallisesti raskasta ja mitä pidempi hajautusarvo on, sitä vaikeampi väsytyshyökkäystä on toteuttaa.

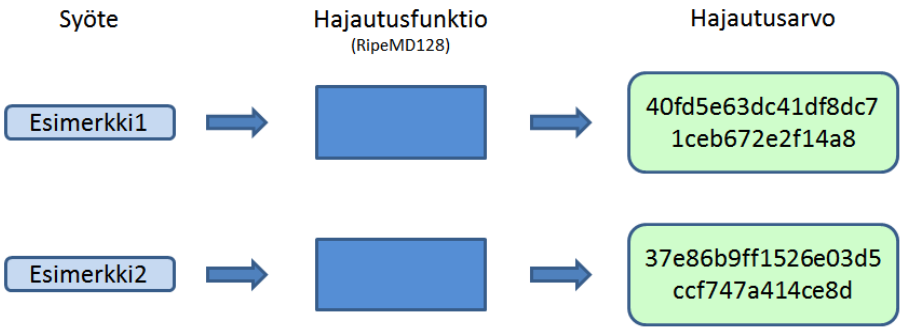


Kuva 1. Eripituisten syötteiden käsittely hajautusfunktiolla

Kuten kuvasta 1 näkee, hajautusfunktio tuottaa aina samanpituisen hajautusarvon riippumatta syötteen pituudesta. Hajautusarvon pituus riippuu käytettävästä hajautusfunktiosta: kuvan 1 esimerkissä käytetty hajautusfunktio (RipeMD128) tuottaa nimensä mukaisesti 128 bittiä pitkän hajautusarvon.

Hajautusarvot ilmaistaan useimmiten heksadesimaalisina merkkijonoina, ts. niissä käytetään numeroita nollasta yhdeksään ja lisäksi kirjaimia pienestä a:sta pieneen f:n. Siten 128-bittinen hajautusarvo muodostaa 32 heksadesimaalimerkkiä pitkän merkkijonon kun jokainen merkki vastaa neljää bittiä.

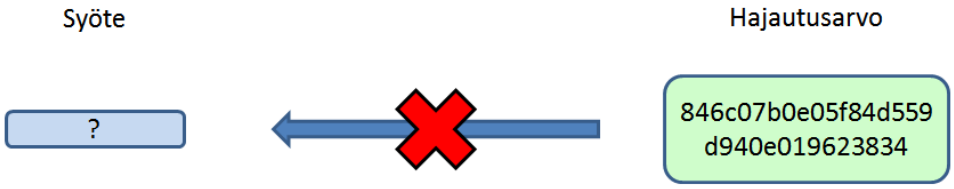
Kuten kuva 1 osoittaa, vaihtoehtoinen suomenkielinen termi ”hash value” –sanalle, tiiviste, voisi olla harhaanjohtava: jos syöte on lyhyempi kuin tiivisteen pituus tietoa ei niinkään tiivistetä kuin koodataan. Useimmiten tiivisteen syöte on kuitenkin huomattavasti tiivistettä pidempi merkkijono tai tieto, jolloin tiiviste on luonnollisestikin alkuperäistä dataa lyhyempi.



Kuva 2. Pienten syötemuutosten vaikutus hajautusarvoon

Kuvassa 2 korostetaan hajautusfunktion toista hyödyllistä ominaisuutta: pienetkin muutokset syötteessä tuottavat aivan erilaiset hajautusarvot. Esimerkissä yhden merkin muuttaminen tuottaa hyvin erilaisen hajautusarvon.

Yhdessä kuvien 1 ja 2 esimerkit osoittavat, miksi hajautusarvoja käytetään runsaasti kryptografiassa ja salauksessa: lopullisesta hajautusarvosta ei voida päätellä mitään alkuperäisestä syötteestä, kuten kuva 3 tiivistää.



Kuva 3. Tiivisteestä ei voida päätellä syötettä

Useimmiten käytettyjä hajautusfunktioita ovat SHA-pohjaiset, NSA:n kehittämät hajautusalgoritmit, joista vanhin (SHA-1) on siirtymässä turvattomuutensa takia pois käytöstä ja sitä korvaavat SHA-2 ja SHA-3 standardit. (NIST 2015.) Esimerkiksi Bitcoinin käyttämä SHA256^2–hajautusalgoritmi kuuluu juurikin SHA-2–standardin mukaisiin hajautusalgoritmeihin.

2.3 **Työn osoitus**

Työn osoituksella (Proof-of-work) tarkoitetaan työtä, joka on tietokoneelle laskennallisesti raskasta. Esimerkiksi ns. CAPTCHA-tekstintunnistuskentät ovat työn osoitusta: ihmisen on helppo tunnistaa niiden sisältämät merkkijonot, mutta toistaiseksi tietokoneen on raskas erottaa merkkejä.

Kuva 4. Esimerkkejä erilaisista CAPTCHA-teksteistä. (Phillips 2015.)

CAPTCHAssa ihminen tekee työn (tulkitsee kuvan sisältämän merkkijonon) ja täten osoittaa, ettei ole tietokone, jolta työ kestäisi toistaiseksi huomattavasti pidempään. Työn osoituksella voidaan torjua esim. automatisoituja hyökkäyksiä sillä tietokone joutuu käyttämään paljon laskentatehoa työn osoituksen suorittamiseen. (Franco 2015, 102-103.)

Työn osoituksen lisäksi lohkoketjujen suojauksessa on harkittu muita menetelmiä kuten osakkuuden osoitus (proof-of-share), polton osoitus (proof-of-burn) että ajan osoitus (proof-of-time). Toistaiseksi työn osoitus on kuitenkin käytetyin menetelmä. (Franco 2015, 233-237.)

Työn osoitus voidaan suorittaa usealla eri algoritmilla painottaen esimerkiksi muistirasittavuutta kuten Litecoinin käytttämä scrypt-kirjasto tai prosessorirasittavuutta kuten hajautusarvoratkonnassa. (Litecoin 2014.)

2.4 **Louhinta**

Louhinta (mining) on menetelmä, jolla lohkoketjun lohkot sidotaan toisiinsa. Louhija suorittaa työn osoituksen, joka allekirjoittaa lohkon ja sitoo sen sisältämän tiedon edellisen lohkon tiivisteen kanssa lohkoketjun viimeiseksi. Vaihtoehtoisissa lohkoketjutoteutuksissa, joissa työn osoitus on korvattu toisella tavalla varmentaa lohko, myös louhinnan nimi on muutettu, esim. painamiseksi tai lyömiseksi (minting). (Franco 2015, 173-174.)

Louhinnan toteuttamisen tarkemmat määrittelyt ovat lohkoketjua toteuttavassa ohjelmistossa, mutta yleisesti ottaen louhinta tapahtuu seuraavassa järjestyksessä:

1. Louhija saa vertaisverkosta uusimman lohkoketjuun lisätyn lohkon tiedot.
2. Louhija tarkistaa, että lohkon sisältämä tieto on validia ja lohkoketjun määritysten mukaista ja työn osoituksen täyttävän lohkoketjun vaatimukset.
3. Jos kohdan 2 ehdot eivät täyty, uusin lohko hylätään, sitä ei lisätä lohkoketjuun ja louhija jatkaa uuden lohkon louhimista.
4. Louhija valitsee tiedot, joita haluaa lisätä lohkoon.
5. Louhija alkaa suorittaa laskutoimitusta työn osoitukseksi.
6. Jos vertaisverkosta tulee ilmoitus uudesta hyväksytystä lohkosta, suoritetaan kohdan 2 tarkistukset.
7. Jos tarkistus kohdassa 6 hyväksytään, aloitetaan työn osoitus alusta uusimman lohkoketjun tietojen perusteella.
8. Jos uusin lohko ei läpäise tarkistusta, jatketaan louhimista.
9. Kun saadaan vaatimukset täyttävä työn osoitus, lohko tietoineen lähetetään eteenpäin vertaisverkon hyväksyttäväksi ja uutta lohkoa voidaan alkaa louhia viimeisimmän lohkon jatkoksi.

Koska louhinta on niin oleellinen osa lohkoketjun toimintaa, louhija saa lohkon valmistumisesta palkkion, esim. Bitcoinin tapauksessa bitcoineja. Louhijoilla on myös valta päättää, mitä tietoa he louhimaansa lohkoon sisällyttävät. Vaikka kirjattavia tapahtumia ei olisi, louhija voi louhia tyhjän lohkon saaden silti palkkion louhinnasta. Tyhjäkin lohko vahvistaa kuitenkin koko ketjun turvallisuutta. (Nakamoto 2008, 4.)

Lohkoketjujen haarautumista syntyy, kun useampi vertaisverkon solmu ratkaisee työn osoituksen samanaikaisesti tai ajallisesti niin lähellä toisiaan että lohko ei ehdi levitä koko vertaisverkkoon. Tätä tapahtuu sitä enemmän, mitä suurempi lohkoja ratkova verkko on ja mitä alhaisempi on vaikeusaste lohkon louhimiseen vaadittavalta työn osoitukselta.

Mahdolliset ristiriidat lohkoketjussa ratkaistaan dynaamisesti: lyhyempi lohkoketju, ts. se johon on louhittu vähemmän uusia lohkoja, hylätään ja sen lohkojen tiedot pitää louhia uudestaan jotta ne tulevat lisätyiksi lohkoketjuun. Koska vertaisverkon solmut louhivat koko ajan uusia lohkoja, käytännössä laskentateho ja etäisyydet verkon solmujen välillä ratkaisevat mitkä lohkoketjut ovat osa virallista lohkoketjua. (Nakamoto 2008, 3-4.)

Lohkoketjun murtaminen on sitä hankalampaa, mitä useampia lohkoja ketjussa on: koska uudet lohkot sisältävät aina edellisen lohkon hajautusarvon, lohkoon tallennetun tiedon muuttaminen vaatisi kaikkien lohkoketjussa sen jälkeen sijaitsevien lohkojen tietojen murtamista ja saattamista lohkoketjuun. Samanaikaisesti kuitenkin uusia lohkoja lisätään, joten murtaakseen lohkoketjun hyökkääjällä täytyisi olla käytössään koko vertaisverkkoa suurempi laskentakapasiteetti. Tämän vuoksi hyökkäyksiä kutsutaan hieman harhaanjohtavasti 51 % -hyökkäyksiksi. (Franco 2015, 113.)

3 VIRTUAALIVALUUTTA BITCOIN

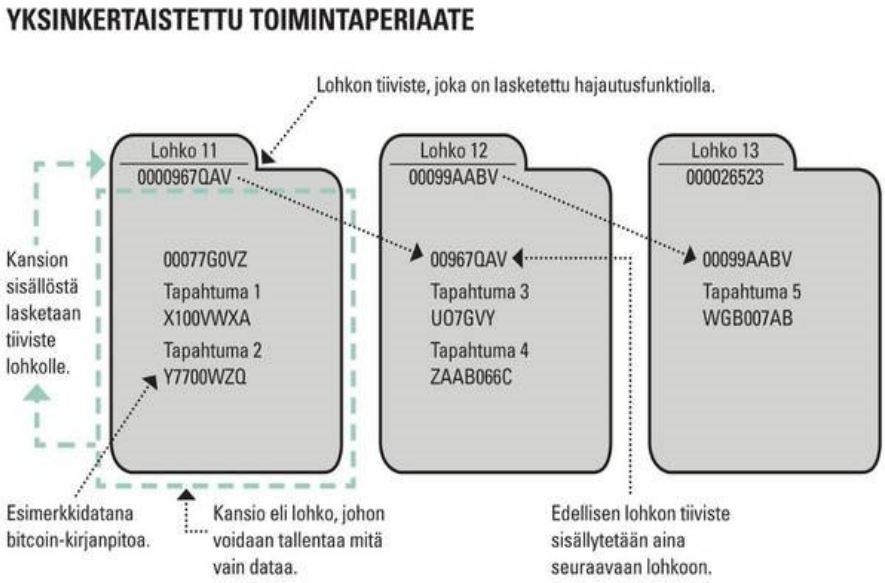
Toistaiseksi tunnetuin ja yleisin lohkoketjuja käyttävä sovellus on Bitcoin-virtuaalivaluutta, lohkoketjuteknologiahan luotiin Bitcoinia varten. Bitcoin käyttää omaa lohkoketjuaan virtuaalisena pääkirjanaan, vertaisverkko-protokollana omaa bitcoin-protokollaansa ja työn osoituksena hajautus-funktiota, joka laskee lohkosta hajautusarvon tietyllä määrällä alkunollia. Alkunollien määrä ja sen perusteella työn vaikeus määräytyy koodissa dynaamisesti siten, että lohkoja syntyy haluttu määrä, n. lohko kymmenessä minuutissa. (Bitcoin 2017.)

Uusia bitcoineja syntyy, kun louhija suorittaa työn osoituksen. Saatujen bitcoinien määrä riippuu ajasta. Bitcoinin alkuaikoina (2008) lohkosta sai 50 bitcoinia, nykyään (toukukuussa 2017) 12.5 bitcoinia. Tämä määrä, louhimispalkkio, puolittuu aina noin neljän vuoden välein. Tämä raja on määritelty suoraan Bitcoinin lähdekoodiin. (Bitcoin 2017.)

Bitcoinien omistajuus on aina sidottu osoitteeseen: se joka hallitsee osoitetta ja siihen liittyvää yksityistä avainta hallitsee osoitteeseen liitettyjä bitcoineja ja voi siirtää niitä toisiin osoitteisiin. Yhdellä henkilöllä voi olla hallussaan monta osoitetta ja niihin liittyviä bitcoineja, ja hän voi siirrellä bitcoinejaan omien osoitteidensa välillä pitääkseen henkilöllisyytensä paremmin piilossa.

Jokainen bitcoin-lohko sisältää edellisen lohkon hajautusarvon, kertakäyttöisen arvon (nonce) ja mahdollisesti yhden tai useampia transaktioita. Transaktiot on allekirjoitettu ja bitcoin-vertaisverkon solmu tarkistaa allekirjoitukset ja työn osoituksen ennen kuin jakaa lohkoa eteenpäin bitcoin-verkossa. Kertakäyttöinen arvo on työn osoitus: louhija kokeilee erilaisia arvoja kunnes löytää arvon, jolla lohkon tiiviste sisältää tarvittavan määrän alkunollia.

Asiaa selventää alla oleva kuva 5, joka esittelee yksinkertaistetun lohkoketjun toimintaperiaatteineen. Kuvan lohkojen sisältämä esimerkkidata on yksinkertaistettu, mutta lohkon ja lohkoketjun rakenne selviää siitä hyvin.



Kuva 5. Yksinkertaistettu lohkoketju. (Tivi 2016.)

On myös mahdollista louhia ”tyhjä” lohko, ts. lohko joka ei sisällä transaktioita. Koska lohkon louhinta tuottaa louhijalleen tuottoa, Bitcoineja, tyhjien lohkojen louhimista pyritään karsimaan jättämällä maksutapahtumiin louhijaa varten pieni korvaus. (Franco 2015, 154.)

Lohkoketjun haarautumistilanteet ratkaistaan Bitcoinissa vertailemalla kilpailevien haarojen työn todisteen vaikeusasteita. Suuremman vaikeusasteen ketju voittaa ja hylättyjen lohkojen sisältämät transaktiot palautetaan vapaiksi uusia lohkoja varten. (Bitcoin 2017; Nakamoto 2008, 3.)

Bitcoinissa tunnistautuminen tapahtuu julkisen avaimen järjestelmää käyttäen. Tavoitteena ja suosituksena on että jokainen bitcoin-tapahtuma liittyy eri osoitteeseen. Osoite muodostetaan julkisesta avaimesta lisäämällä siihen tarkistussummia ja ajamalla se usean hajautusfunktion läpi. Tapahtuma varmennetaan yksityisellä avaimella. (Bitcoin 2017.)

Bitcoin on pseudonyymi valuutta. Pseudonyymiys tarkoittaa tässä yhteydessä sitä, että vaikka yksittäisen bitcoin–osoitteen omistajaa ei tiedetä, se voidaan päätellä osoitteen tekemistä maksuista, sillä kaikki maksut ovat aina julkisia. Juuri yksityisyyden suojaamiseksi suositellaankin useampien osoitteiden käyttöä.

Koska bitcoin-osoitteita suositellaan käytettäväksi vain kerran, bitcoinin käyttö käytännössä edellyttää lompakko-ohjelmiston (bitcoin wallet) käyttöä. Lompakko on ohjelma, joka generoi ja hallinnoi bitcoin-osoitteita ja niihin liittyviä bitcoineja sekä mahdollistaa bitcoinien lähettämisen ja vastaanottamisen. Lompakko myös sisältää käyttäjän bitcoinien-osoitteisiin liittyvät salaiset avaimet.

4 BITCOININ PERILLISET

Koska Bitcoin on avoimen lähdekoodin järjestelmä, siitä on helppoa ja laillista luoda uusia variaatioita. Näitä variaatioita kutsutaan nimillä alt-coin tai metacoin, kaupallisemmissa yhteyksissä käytetään myös termejä Blockchain 2.0 tai jopa Blockchain 3.0. (Swan 2015, 15, 21.)

Monimutkaisen termistön takana on sekä ideologisia eroja että halu erottaa lohkoketjuja pelkistä virtuaalivaluuttatoteutuksista yleensä ja Bitcoinista erityisesti.

Näissä Bitcoinin variaatioissa on sekä uusia virtuaalivaluuttoja että muita toteutuksia, kuten keskittämättömien sovellusten ajamiseen tarkoitettu Ethereum ja digitaalisten omistusten varmistamiseen suunniteltu Colored Coins. (Swan 2015, 15, 21.)

Bitcoin ja siitä haarautuneet projektit ovat vielä tuoreita. Tästä johtuen käsitteistö on vielä hieman epäselvää ja vakiintumatonta. Tässä opinnäytetyössä käytettävien termien altcoin, metacoin ja Blockchain 2.0 määrittelyt löytyvät alta. Määrittelyt saattavat erota joidenkin lähteiden käyttämien määrittelyjen kanssa.

Toukokuun lopussa 2017 rahallisesti arvokkaimmat lohkoketjutoteutukset olivat Bitcoin ($35,547,022,114), Ethereum ($15,781,258,742), Ripple ($8,828,509,454), NEM ($1,928,311,817), Ethereum Classic ($1,559,277,507) ja LiteCoin ($1,301,965,893). Seuraavaksi arvokkain kryptovaluutta, Dash, jäi alle miljardin dollarin rajan n. 800 miljoonan dollarin arvolla. (CoinMarketCap 2017.)

Kaiken kaikkiaan erilaisia lohkoketjuratkaisuja on toukokuun lopussa 2017 runsaasti, virtuaalivaluuttoja yli 700 ja blockchain 2.0 – toteutuksiakin yli 100 erilaista (CoinMarketCap 2017.)

4.1 Alt-coins

Altcoineiksi kutsutaan Bitcoinista täysin erillisiä toteutuksia tai haaraumia Bitcoinin lähdekoodista. Koodin haarautumisen (forking) mahdollistaa Bitcoinin avoimeen lähdekoodiin perustuva rakenne. (Franco 2015, 194.)

Altcoineilla on oma lohkoketjunsa. Niissä lohkon varmistamiseen käytetty menetelmä on usein valittu joko eri hajautusfunktiota käyttäväksi työn osoitukseksi (esim. Litecoin ja scrypt-algoritmi Bitcoinin SHA256^2-algoritmin sijaan) tai korvattu työn osoituksen esim. osakkuuden osoituksella.

Altcoinien haarautumisen taustalla on usein ideologisia syitä: esimerkiksi tarve tehdä aidosti anonyymi valuutta Bitcoinin pseudonymiteetin sijaan tai halu tehdä louhinnasta kannatettavaa myös satunnaisille käyttäjille.

Yksi suosituista altcoineista on LiteCoin, joka on kuudenneksi arvokkain lohkoketjutoteutus. Litecoinin käyttämä scrypt-hajautusalgoritmi valittiin, koska se kuluttaa paljon muistiresursseja toisin kuin esim. Bitcoinin käyttämä SHA256^2-algoritmi, joka käyttää runsaasti laskentatehoa. (Litecoin 2014.)

Muistin käytön korostaminen prosessoritehon sijaan mahdollistaa paremmin tavallisten käyttäjien suorittaman louhinnan, kun taas Bitcoinin louhinta on siirtynyt suurelta osin isoille toimijoille, joille on varaa ostaa laskentatehoa (ja hajautuslaskentaan sopivia erikseen suunniteltuja mikropiiriratkaisuja) vain louhintaa varten.

4.2 **Metacoins**

Metakolikoksi (metacoin) kutsutaan lohkoketjutoteutusta, joka käyttää bitcoinin lohkoketjua ja lisää sen päälle omaa toiminnallisuuttaan. Tämä on mahdollista, koska bitcoin-protokolla ei ota mitenkään kantaa lohkoketjussa tapahtuvan ”ylimääräisen”, ei bitcoin-transaktioihin, liittyvän tiedon siirtoon. Bitcoin-protokollassa on jopa kenttä tällaisen metatiedon siirtoon (OP_RETURN). (Franco 2015, 171; Bitcoin n.d.)

Metakolikon toteuttava ohjelmisto tarkkailee näitä lisättyjä tietoja ja toimii niiden perusteella, kun taas Bitcoin ohittaa ne. Näin ohjelmat voivat toimia rinnakkain, kunhan louhittavat metakolikot toteuttavat myös Bitcoinin vaatimukset. Luonnollisesti vain metakolikko-ohjelmistot osaavat louhia metakolikoita, mutta ne sijoittuvat Bitcoinin lohkoketjuun siinä missä tyhjät Bitcoin-lohkotkin.

Bitcoinin lohkoketjua käytetään sen takaaman turvallisuuden vuoksi, lohkoketjujen turvallisuus kun lisääntyy suhteessa lohkojen määrään. Bitcoinin yleisyys on yksi suurimmista tekijöistä Bitcoinin suosiosta metacoinien pohjana.

Metacoinit eivät ole kasvattaneet suosiotaan yhtä paljon kuin altcoinit, esimerkiksi Omni (entiseltä nimeltään Mastercoin) on vasta 97. arvokkain lohkoketjutoteutus (CoinMarketCap 2017.) Muita metacointoteutuksia ovat esimerkiksi em. Colored Coins ja OpenAssets.

4.3 **Blockchain 2.0**

Blockchain 2.0 on yleiskäsite Bitcoinia seuranneille lohkoketjutoteutuksille, jotka ovat muutakin kuin kryptovaluuttoja, kuten digitaalisten omistusten turvaamiseen perustuvat lohkoketjut (esim. Decent) tai automatisoidut toimijat (esim. Ethereum.)

Merkittävin seuraavan sukupolven lohkoketjutoteutus on tällä hetkellä Turing-täydellinen Ethereum, joka on suunniteltu toteuttamaan keskittämättömiä ohjelmointiratkaisuja ja älysopimuksia. Turing-täydellisyys tarkoittaa sitä, että Ethereumilla voidaan suorittaa mikä tahansa tietokoneohjelma. (Swan 2015, 21.)

Ethereum on myös hyvä esimerkki lohkoketjujen hajaannuksesta: Ethereum-projekti on jo jakaantunut kahtia Ethereumiin ja Ethereum Classiciin. Ethereum Classic irtaantui alkuperäisestä Ethereumista heinäkuussa 2016 ilmoittaen syyksi Ethereumin tekemät koodipohjan muutokset, etenkin mahdollisuuden muuttaa lohkoketjun sisältöä jälkikäteen. (Ethereum Classic 2016, 2.)

Älysopimuksilla tai älykkäillä sopimuksilla (smart contracts) tarkoitetaan lohkoketjujen yhteydessä transaktioita, jotka toteutuvat vain tiettyjen ehtojen täyttyessä. Esimerkiksi älykäs sopimus voisi olla vaikkapa sopimus, joka sallii palvelimen levytilan vähetessä palvelimen ostaa lisää levytilaa pilvipalvelusta Bitcoineilla.

Joissakin yhteyksissä käytetään jo termiä Blockchain 3.0, mutta kun termi Blockchain 2.0 on yhä avoin ja sen sisältämät konseptit kehitys- tai testausvaiheessa, seuraavasta sukupolvesta puhuminen lienee ennenaikaista. (Swan 2015, 27; vrt. Franco 2015, 183.)

5 LOHKOKETJUJEN KÄYTTÖKOHTEET

Asioiden internet (IoT, Internet of Things) on jatkuvan tutkimuksen kohteena oleva ja alati kasvava tietotekniikan osa-alue. Sen haasteena ovat kuitenkin olleet tietoturvaongelmat.

On mahdollista että näitä tietoturvaongelmia voitaisiin lähteä ratkaisemaan lohkoketjujen avulla. Rekisteröimällä esineiden omistajuus lohkoketjuun, voitaisiin estää asiattomien käyttäjien toimet. Kuten edellä osoitettiin, lohkoketjun turvallisuus kasvaa sen lohkojen määrän myötä, joten toisin kuin tavanomaisissa ratkaisuissa, turvallisuus vain lisääntyy ajan myötä.

Kotimaassa Sovelton johtama konsortio tutkii ja kehittää asioiden internetiä ja lohkoketjuja käyttävää Thing2Data-hanketta. Hankkeessa on mukana merkittäviä toimijoita kuten Liikennevirasto, Liikenne- ja viestintäministeriö, Microsoft, Tieto ja VR Group. (Sovelto 2016.)

Thing2Data-hankkeessa yhdistetään älylaitteita ja internetiin liittymättömiäkin laitteita. Esineisiin liittyvää käyttölogiikkaa tai tietoja sijoitetaan verkkoon ja esine ja tieto/logiikka yhdistetään, joko jo olemassa olevien tunnisteiden (kuten vaikkapa rekisterikilpien) tai palvelun generoimien tunnisteiden pohjalta. Lohkoketjuja käytetään hankkeessa säilyttämään turvallisesti tietoja, jolla tunniste ja palvelu liitetään toisiinsa. (Sovelto 2016.)

Thing2Data-hankkeen kaltaisia IoT- ja lohkoketjuteknologioita yhdistäviä hankkeita ovat myös Catenis ja Chronicled, jotka tarjoavat rajapintoja tiedon luotettavaan säilyttämiseen lohkoketjussa (Catenis 2016; Chronicled n.d.)

Rahoitusala on myös kiinnostunut lohkoketjuista. Rahoitusalalla kiinnostus on virtuaalivaluuttojen lisäksi lohkoketjujen käytöstä kansainvälisissä tilisiirroissa ja arvo-osuuskaupassa ja siihen liittyvissä rekisteröinneissä. R3-konsortio, johon kuuluu 70 suurta rahoitusalan toimijaa, on perustanut ja kehittää Corda-nimistä lohkoketjuratkaisua rahoitusalan tarpeisiin (R3 n.d.)

Valtiot ovat toteuttamassa useita lohkoketjuprojekteja. Viro on ilmoittanut tavoitteekseen varmentaa terveystiedot lohkoketjujen avulla, Georgia luo lohkoketjuihin perustuvaa kiinteistörekisterijärjestelmää ja Honduras pyrkii maarekisterin lohkoketjuttamiseen. (Honkanen 2017, 29-32.)

Alankomaissa on toteutettu vuonna 2016 11 pilottiprojektia, joilla testattiin lohkoketjujen soveltuvuutta yhteiskunnan eri aloilla. Projektit sisälsivät mm. digitaalisen identiteetin kehittämistä, terveydenhuollon suostumusten varmistamista ja veronkannon tehostamista. Neljä projekteista etenee seuraavaksi prototyyppivaiheeseen. (Blockchain Pilot 2017.)

Energiasektori on kiinnostunut sähkönmyynnistä ja –ostosta älykkäiden sopimusten avulla, mutta toistaiseksi kaikki projektit ovat suunnitteluasteella. (Honkanen 2017, 13-14.)

Media-alalla lohkoketjuja tutkitaan digitaalisten sisältöjen myynnissä ja digitaalisten oikeuksien varmentamisessa. Tässä toistaiseksi merkittävin toimija on Decent, joka kehittää lohkoketjuilla toimivaa media-alustaa, jonka se lupaa estävän piratismin. (Decent n.d.)

Microsoft, Phillips ja Tierion yhdessä muiden toimijoiden kanssa kehittävät Chainpoint-standardia, joka säilöö Bitcoinin ja Ethereumin lohkoketjuihin tiedostojen tai prosessien aikaleimoja. Tässäkin lohkoketjua käytetään tiedon turvallisuuden ja muuttamattomuuden varmistamiseksi. (Chainpoint n.d.)

Steem on sosiaalisen median sivusto, jossa käyttäjä saavat julkaisuistaan sekä Steemin omaa kryptovaluuttaa (joka on vaihdettavissa rahaksi) että eräänlaista vaikutusvaltaa, Steem Poweria. Steem power määrittää kuinka paljon annettu ääni (ylös- tai alasäänestys) vaikuttaa julkaisun saamaan valuuttaan. Tarkoituksena on palkita sisällöntuottajia rahallisesti ja tuottaa keskittämätön, sensuroimaton sosiaalisen media alusta. (Larimer et al. 2017.)

Parviälyä ja älykkäitä sopimuksia yhdistämään on suunniteltu heinäkuussa 2017 vielä betavaiheessa oleva Augur, joka käyttää alustanaan Ethereumia. Augurissa käyttäjät sijoittavat virtuaalisia osakkeita sen perusteella, miten arvelevat tosimaailman tilanteiden kehittyvän. Henkilö voi esimerkiksi sijoittaa osakkeitaan sille, että Leonardo DiCaprio voittaa toisen Oscarin. Oikeasta arvauksesta palkitaan lisäosakkeilla. Augurin toiminta pohjautuu teorialle, että suurten ihmismassojen valinnat ennustavat tapahtumia paremmin kuin yksittäisten asiantuntijoiden näkymykset. (Augur n.d.)

Hyperledger on Linux Foundationin johtama yhteistoimintahanke, joka pyrkii kehittämään avoimen lähdekoodin lohkoketjuympäristön. Hankkeessa ovat mukana mm. Fujitsu, IBM, Intel ja Samsung. Hanke keskittyy aluksi talouden ja terveydenhuollon pariin, seuraavassa vaiheessa mukaan tulevat jakeluketjun tarpeisiin kehitettävät ohjelmistot. (Hyperledger n.d.)

6 LOHKOKETJUTUTKIMUS

Kotimainen tutkimus lohkoketjuista on vielä vähäistä, mutta tutkimusprojekteja on koko ajan käynnissä ja niiden tuloksia voidaan odottaa lähiaikoina.

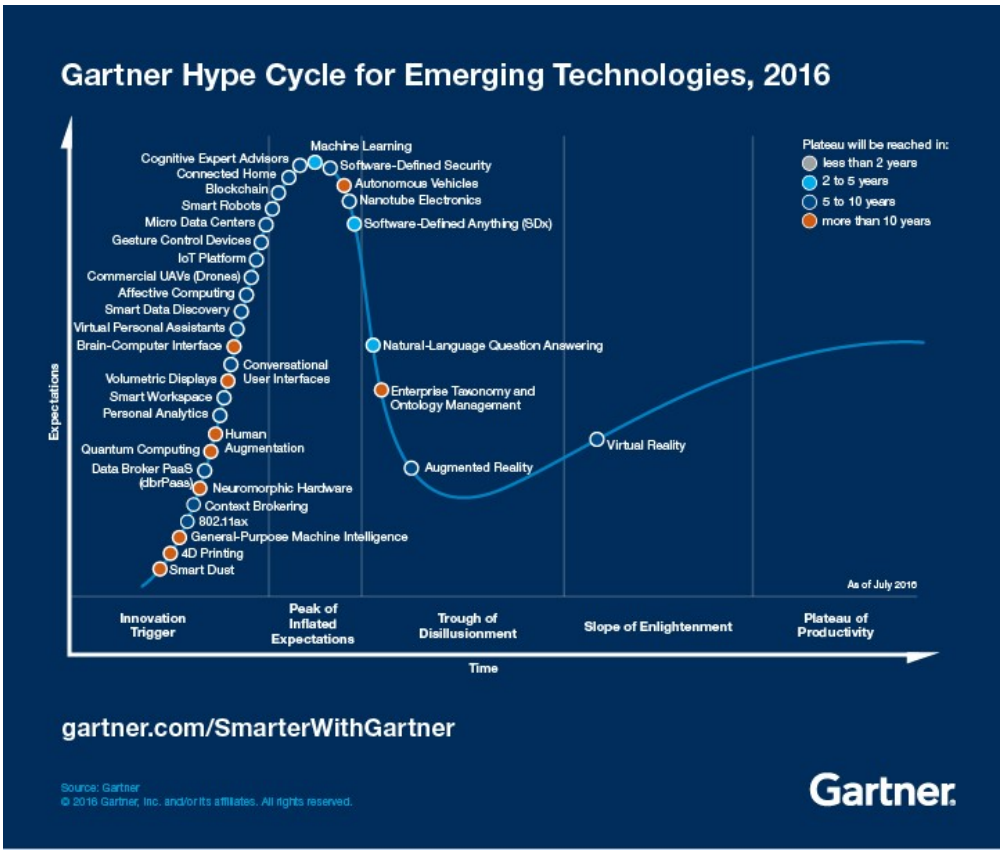
Tommi Laine tutki kandidaatintyössään lohkoketjujen soveltamista pankkien välisissä tilisiirroissa. Laineen mukaan lohkoketjut eivät ole vielä teknisesti valmiita tilisiirtojen korvaamiseen vaikkakin tilisiirtojen teknologinen kehittäminen on tärkeä kehityskohde. Lohkoketjujen potentiaalinen merkitys on silti Laineen mukaan iso, vaikkakin lohkoketjujen käytön vakiintuminen finanssisektorilla on vielä epävarmaa. (Laine 2017, 31-32.)

ETLA on julkaissut raportin Ethereumiin perustuvasta prototyypistä, joka hyödyntää älykkäitä sopimuksia ja mahdollistaa sähkön myynnin ja oston suoraan osapuolien välillä ilman keskitettyä kauppapaikkaa. Prototyyppi on kehitetty yhdessä teollisuuden kanssa ja odottaa jatkokehitystä ja testausta. Lainsäädäntö ja muu säätely ovat epävarmuustekijöitä, joitten vaikutusta ei vielä tunneta. (Hukkinen et al. 2017, 4.)

Kattavin kotimainen raportti lohkoketjuista on Petri Honkasen raportti, joka pyrkii selvittämään lohkoketjujen käyttöä. Honkanen esittelee laajaalaisesti mutta lyhyesti lohkoketjun hyödyntämiseen tähtääviä tahoja ja yleisimpiä lohkoketjutoteutuksia (Honkanen 2017, 6, 9-11.)

EU-parlamentti on käsitellyt lohkoketjuja ja lausumassaan toteaa pitävänsä virtuaalivaluuttoja ja lohkoketjuja positiivisena asiana kansalaisille ja talouskehitykselle, mutta on huolissaan riskeistä ja lainsäädännön kehittämisestä. Parlamentti perusti työryhmän seuraamaan kehitystä ja selvittämään tarvittavaa säätelyä sekä tiedottamaan asiaan liittyvistä mahdollisuuksista ja riskeistä. (EU-parlamentti 2016.)

Euroopan komission yhteinen tutkimuskeskus (The Joint Research Center) on käynnistänyt huhtikuussa 2017 #Blockchain4EU-hankkeen, joka kartoittaa lohkoketjujen sovelluksia, etsii käyttökohteita lohkoketjuratkaisuille ja selvittää mahdollisia lainsäädännöllisiä tarpeita. (EU Policy Lab n.d.)



Kuva 6. Arvio teknologioiden tulevaisuuskehityksestä (Gartner 2016.)

Kansainvälinen ICT-alan tutkimus- ja konsultointiyritys Gartner antaa vuosittaisia arvioraportteja ICT-alan ja siihen liittyvien teknologioiden tulevaisuuskehityksestä. Gartner jakaa teknologioihin liittyvät odotukset viiteen vaiheeseen (kuva 6): innovaatiosysäys (Innovation Trigger), ylimitoitettujen odotusten huippu (Peak of Inflated Expectations), pettymysten aallonpohja (Trough of Disillusionment), valaistuksen rinne (Slope of Enlightenment) ja tuottavuuden tasanko (Plateau of Productivity). Tämän lisäksi teknologioista arvioidaan millä aikavälillä niiden arvioidaan saavuttavan em. tasanko. (Gartner 2016.)

Gartnerin mukaan lohkoketjut ovat lähestymässä huippukohtaa alun innovaatiosysäksen jälkeen, ja edessä on pettymysten täyttämä vaihe kunnes lohkoketjujen hyödyt alkavat realisoitua ja niihin sijoitetut resurssit alkavat kannattaa. Gartner ennustaa tämän tapahtuvan vasta 5–10 vuoden kuluessa.

World Economic Forumin Global Agenda Council julkaisee myös raportteja teknologian kehityksestä ja sen haasteista. Tulevaisuusraportissaan WEF arvioi että 2027 on käännekohta, jossa 10 % globaalista bruttokansantuotteesta on varastoituna lohkoketjuihin, ja 58 % vastaajista uskoo sen tapahtuvan jo 2025 mennessä. (World Economic Forum 2015.)

Eduskunnan tulevaisuusvaliokunta seuraa myös teknologioiden kehittymistä. Viimeisimmässä selonteossaan 2016, jossa seurataan edellisen, 2013 julkaistun raportin jälkeen tapahtuneita muutoksia teknologia-alalla lohkoketjut ovat vasta seurannassa ja niille suositellaan omaa kategoriaa. Raportin mukaan lohkoketjut ovat jatkuvasti laajeneva alue, jolla arvioidaan olevan suuri vaikutus hallinnon rationalisointiin ja perinteisten organisaatioiden valta- ja valvontarakenteiden ohittamiseen. (Linturi 2016, 114-115.)

Näiden asiantuntijoiden näkemysten perusteella voidaan katsoa, että lohkoketjut ovat lupaava ala, jonka vaikutus tosin ei ole huomattava vielä lähivuosien aikana. Raportit ennustavat positiivista kehitystä, mutta niiden antama kuva on hyvin erilainen median välittämään hehkutukseen nähden.

7 LOHKOKETJUJEN HAASTEET

Lohkoketjujen arkipäiväistymisen tiellä on vielä monenlaisia esteitä. Yksi hidastava tekijä on avoimen lähdekoodin ohjelmistoprojektien taipumus haarautua useiksi eri projekteiksi.

Yksi syy haarautumiseen ovat ideologiset syyt, kuten esimerkiksi jako Ethereumin ja Ethereum Classicin välillä. Hajaannuksen syynä on ennen kaikkea erimielisyys siitä, pitääkö lohkoketjuun säilötyn tiedon olla pysyvä vai pitääkö sitä voida muuttaa esim. inhimillisten koodi- tai logiikkavirheiden takia (Ethereum Classic 2016.)

Myös erimielisyydet teknisissä toteutuksissa voivat olla syinä, kuten Bitcoinin ja Litecoinin välillä: toteutetaanko työn osoitus prosessoritehoa vaativalla vai muistikapasiteettia vaativalla algoritmilla (Litecoin 2014.)

Loppukäyttäjän kannalta syyt haarautumiseen ovat kuitenkin yhdentekevät ja lähinnä monimutkaistavat tavallisten käyttäjien siirtymistä virtuaalivaluuttoihin. Bitcoinin yleisyys on vielä toistaiseksi sen etu, mutta on mahdotonta arvioida miten ja milloin siirtyminen edistyneempään virtuaalivaluuttaan tulee tapahtumaan.

Kuten teknologiassa usein, myös lohkoketjuilla on edessään darwinistinen vaihe, jossa vahvimmat tai suosituimmat ratkaisut jäävät eloon ja kehittyvät ja suuri osa karsiutuu tai kuihtuu pois.

Lohkoketjuja voisi verrata selaimiin: niiden markkina-osuus on muuttunut jatkuvasti uusien selainten vallatessa tilaa vanhoilta. Tammikuun 2009 alussa Internet Explorerin markkinaosuus oli 64,97 %, Firefoxin 26,85 % ja Chromen 1,37 %. Vuoden 2016 joulukuun lopussa osuudet olivat IE 4,44 %, FF 6,72 % ja Chrome 51,06 %. (Statcounter n.d.a.; Statcounter n.d.b.)

Selaimet kehittyivät verkkosivujen kehityksen rinnalla. Määräävä markkina-asema muuttui, jos selaimen kehitys ei pysynyt muun kehityksen mukana. Vielä on hankala ennustaa, onko Bitcoin IE ja Ethereum Firefox ja mikä on tuleva haastaja, Chrome. Varmaa on vain, että seuraavan sukupolven teknologiat syrjäyttävät toteutukset, jotka eivät pysy muutoksessa mukana.

Alankomaiden hallituksen Blockchain Pilot –hankkeessa toteutettiin 11 projektia. Projektien yhteenvedossa todetaan, että suuria lohkoketjuhankkeita ei tässä vaiheessa kannata vielä aloittaa, sillä teknologia on vielä liian kypsymätöntä. Yhteenveto suosittelee sijoittamista seuraavan sukupolven hankkeiden kehittämiseen, riittävään koulutukseen ja sääntöjen ja standardien kehittämistä lohkoketjuhankkeiden tarpeisiin. (Blockchain Pilot 2017.)

Ei pidä myöskään unohtaa lohkoketjun kasvavan kooltaan jatkuvasti. Bitcoinin lohkoketju on elokuussa 2017 kooltaan jo yli 151 gigatavua. Uuden käyttäjän pitää siis joko ladata koko ketju tai luottaa palveluntarjoajiin, joilla on käytössään koko lohkoketju. (CryptoCompare 2017.)

Lohkoketjujen keskittämättömyys on sekä niiden vahvuus että myös riski metacoinien kaltaisissa ratkaisuissa. Projektit, joissa tiedon varmennus tapahtuu esim. Bitcoinin lohkoketjussa ottavat riskin. On mahdollista, että tulevaisuudessa Bitcoinin protokolla muuttuu niin, ettei se salli ylimääräisen tiedon tallentamista lohkoketjuunsa. Syynä tähän voi olla esimerkiksi juuri ym. ketjun koon kasvu. Riskiä voi pienentää käyttämällä rinnakkain useampaa lohkoketjua, kuten esim. Chainpoint tekee.

Teknologian ollessa kansainvälinen myös kansainvälisen lainsäädännön merkitys korostuu: esimerkiksi EU:n General Data Protection Regulation (GDPR) saattaa muodostua esteeksi lohkoketjujen käytölle Euroopassa, sillä se vaatii yksilölle oikeuden poistaa itseään koskevia henkilökohtaisia tietoja siinä missä useimpien lohkoketjujen toteutus taas olettaa että lohkossa oleva tieto on pysyvää ja sitä ei voi muuttaa. Vaikkakin säädöksiin on kirjattu poikkeus pseudonyymille tiedolle, sen tarkkaa määrittelyä ei ole vielä tiedossa. (GDPR Portal n.d.)

On myös naiivia olettaa, että lohkoketjujen taloudellisen merkityksen lisääntyessä verottaja ja muut viranomaiset eivät pyrkisi rajoittamaan ja valvomaan arvonsiirtoja sekä hyötymään virtuaalivaluuttojen käytöstä. Suomessakin verohallinto on todennut virtuaalivaluutoista saatavan tulon (myös louhinnan) olevan veronalaista jo 2013. Toistaiseksi tätä tuloa on kuitenkin mahdotonta valvoa. (Verohallinto 2013.)

8 YHTEENVETO

Lohkoketjuista puhutaan paljon, mutta virtuaalivaluuttoja ja erityisesti Bitcoinia lukuun ottamatta ne ovat toistaiseksi vasta pääosin beta-, prototyyppi- tai proof–of–concept-tasolla. Niiden käyttöönottoa hidastavat niin teknisten ratkaisujen monimuotoisuus ja standardoinnin puute kuin tarvittavan tietotaidon vähyys.

Työn aikana lohkoketjujen toimintaperiaatteet tulivat selväksi, mutta varsinaisia vastauksia lohkoketjujen hyödyntämisestä ei vielä ollut saatavilla. Lohkoketjuja pyritään soveltamaan useilla eri aluille ja potentiaalisia käyttökohteita löytyy paljon, mutta vielä on hankala sanoa mitkä ovat lupaavimpia käyttökohteita ja missä lohkoketjuista on eniten hyötyä.

Lohkoketjujen käyttö on vielä alkutekijöissään ja tulevaisuudessa varmasti kohdataan ongelmia, joihin ei vielä ole osattu varautua. Korvatakseen nykyisiä valuuttoja virtuaalivaluuttojen täytyisi esimerkiksi kyetä kertaluokkaa suurempiin yhtäaikaisiin tapahtumiin. Käytännön kokemuksia näin isoista lohkoketjutoteutuksista ei vielä ole. Valitettavasti, kuten kokemus on osoittanut, täydellinen ongelmatilanteiden ennakointi etukäteen on mahdotonta.

Lohkoketjuihin liittyvän kohun laannuttua ja tilanteen vakiinnuttua toimivimmat ratkaisut ja seuraavan sukupolven lohkoketjutoteutukset tulevat tarjoamaan toimivia ratkaisuja useille elämän eri osa-aluille, mutta millä alueilla ja millä toteutuksilla, on vielä arvailujen varassa.

Vahvimpina ehdokkaina ovat alat, joissa käsitellään suuria tietomääriä useiden, keskenään epäyhteensopivien tietojärjestelmien välillä. Tällaisia aloja ovat esim. terveydenhuolto potilastietoineen, valtiot ja kunnat rekistereineen sekä finanssiala. Näissä lohkoketjujen kaltaiset hajautetut, luotettavat tietokantaratkaisut ovat eniten tarpeeseen.

LÄHTEET

Augur n.d. Augur Documentation. Viitattu 31.7.2017. http://docs.augur.net/#architecture

Bitcoin 2017. Bitcoin source code. Ohjelmiston lähdekoodi. Viitattu 10.4.2017. https://github.com/bitcoin

Blockchain Pilots 2017. Blockchain Pilots: A Brief Summary. Viitattu 1.8.2017. https://docs.wixstatic.com/ugd/df1122_3de6de424d3b4f618af9e768e12d0ca0.pdf

Catenis 2016. Catenis Data Sheet. Viitattu 31.7.2017. Tuotetietodokumentti. http://blockchainofthings.com/downloads/CatenisDataSheet.pdf

Chainpoint n.d. Blockchain proof & anchoring standard. Verkkosivusto. Viitattu 31.7.2017. https://chainpoint.org/

Chronicled n.d. Chronicled FAQ. Verkkosivusto. Viitattu 1.8.2017. https://www.chronicled.com/faq.html

CoinMarketCap 2017. Cryptocurrency market capitalizations. Viitattu 28.5.2017. https://coinmarketcap.com/historical/20170528/

CryptoCompare 5.7.2017. Is the Bitcoin Blockchain too big? Viitattu 31.7.2017. https://www.cryptocompare.com/coins/guides/is-the-bitcoin-blockchain-too-big/

Decent n.d. Blockchain Content Distribution Platform. Verkkosivusto. Viitattu 28.5.2017. https://decent.ch/

Ethereum Classic 20.7.2016. Ethereum Classic Declaration of Independence. Verkkodokumentti. Viitattu 24.5.2017. https://ethereumclassic.github.io/assets/ETC_Declaration_of_Independence.pdf

EU-parlamentti 26.5.2016. Virtual Currencies. Resolution on initiative 2016/2007. Viitattu 28.5.2017. http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2016/2007(INI)#documentGateway

EU Policy Lab n.d. #Blockchain4EU. Verkkosivusto. Viitattu 31.7.2017. http://blogs.ec.europa.eu/eupolicylab/

Franco, P 2015. Understanding Bitcoin. TJ International Ltd, Padstow.

Gartner 19.8.2016. Gartner Hype Cycle for Emerging Technologies. Verkkosivusto. Viitattu 28.5.2017. http://www.gartner.com/smarterwithgartner/3-trends-appear-in-the-gartner-hype-cycle-for-emerging-technologies-2016/

GDPR Portal n.d. Frequently asked questions. Verkkosivusto. Viitattu 31.7.2017. http://www.eugdpr.org/gdpr-faqs.html

Honkanen, P 2017. Lohkoketjuteknologian lupaus. Arcada Working Papers 01/2017.

Hukkinen, T; Mattila, J; Ilomäki, J & Seppälä, T 3.5.2017. A Blockchain Application in Energy. ETLA Reports No 71. https://pub.etla.fi/ETLA-Raportit-Reports-71.pdf

Hyperledger n.d. About Hyperledger. Verkkosivusto. Viitattu 30.7.2017. https://www.hyperledger.org/about

IATE n.d.. Interactive Terminology for Europe, EU:n termitietokanta. Verkkosivu. Viitattu 11.4.2017. http://iate.europa.eu/

Laine, T 2017. Lohkoketjun hyödyntäminen pankkien välisissä tilisiirroissa. LUT School of Business and Management.

Linturi, R 2016. Teknologiamurros 2013-2016. Eduskunnan tulevaisuusvaliokunta, Helsinki.

Litecoin 23.1.2014. Comparison between Litecoin and Bitcoin. Viitattu 28.5.2017. https://litecoin.info/User:Iddo/Comparison_between_Litecoin_and_Bitcoin

Nakamoto, S 2008. Bitcoin: A Peer-to-peer Electronic Cash System. Verkkojulkaisu. Viitattu 11.4.2017. https://bitcoin.org/bitcoin.pdf

NIST (National Institute of Technology) 2015. Secure Hashing. Verkkosivu. Viitattu 13.4.2017. http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html

Phillips, D 2015. Securimage PHP Captcha. Verkkosivu. Viitattu 18.4.2017. https://www.phpcaptcha.org/

R3 n.d. Verkkosivusto. Viitattu 28.5.2017. http://www.r3.com/

Sovelto 13.4.2016. Tavarat älykkäiksi laajan konsortion voimin! Tiedote. Viitattu 31.7.2017. http://www.sovelto.fi/ajankohtaista/tiedotteet/tavarat-alykkaiksi-laajan-konsortion-voimin

Larimer, D & Scott, N & Zavgorodnev, V & Johnson, B & Calfee, J & Vandeberg, M 2017. Steem White Paper. https://steem.io/SteemWhitePaper.pdf

Statcounter n.d.a. Browser Market Share Worldwide 2016. Verkkosivu. Viitattu 1.8.2017. http://gs.statcounter.com/browser-market-share/all/worldwide/2016

Statcounter n.d.b. Browser Market Share Worldwide 2016. Verkkosivu. Viitattu 1.8.2017. http://gs.statcounter.com/browser-market-share/all/worldwide/2009

Tivi 2016. Lohkoketjuteknologia pähkinäkuoressa. Artikkeli. Toimittaja Niclas Storås. Viitattu 19.4.2017. http://www.tivi.fi/Kaikki_uutiset/lohkoketjuteknologia-pahkinakuoressa-tama-kannattaa-tietaa-6537904

TSK ry n.d.. Tietotekniikan termitalkoot, TEPA-termipankki. Verkkosivu. Viitattu 11.4.2017. http://www.tsk.fi/tsk/termitalkoot/fi

Swan, M 2015. Blockchain. O'Reilly Media Inc, Sebastopol.

Valtiovarainministeriö 2008. Valtionhallinnon tietoturvasanasto VAHTI 8/2008. Edita Prima Oy, Helsinki.

Verohallinto 28.8.2013. Virtuaalivaluuttojen tuloverotus. Verohallinnon ohje. Viitattu 31.7.2017. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen_tuloverotu/

World Economic Forum 2015. Technology Tipping Points and Societal Impact. Verkkojulkaisu. Viitattu 28.5.2017. http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf