Haaga-Helia
ammattikorkeakoulu Oy

Blockchain-teknologia ja sen käyttötapaukset energiateollisuudessa

Yousuf Ahmed

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2019

Tiivistelmä

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä(t)
Yousuf Ahmed

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Blockchain-teknologia ja sen käyttötapaukset energiateollisuudessa

Sivu- ja liitesivumäärä
57+7

Blockchain on uusi ja nouseva teknologia, jolla on potentiaalia muuttaa monia tuntemiamme teollisuuden aloja. Blockchain pyrkii muun muassa korjaamaan tietoturva-aukkoja, parantamaan luotettavuutta järjestelmiin ja korjaamaan erinäisiä perinteisissä keskitetyissä tietojärjestelmissä usein esiintyviä ongelmia. Tämä toteutetaan luomalla konsensusta ja luottamusta hajautetussa verkossa kryptografian erilaisten protokollien voimin.

Vaikkakin Blockchain usein mielletään vain Bitcoinia toteuttavana teknologiana, on sillä potentiaalisia käyttötapauksia myös finanssisektorin ulkopuolella. Vaikka Blockchain onkin yksi nousevista teknologioista, on se kuitenkin vielä alkutaipaleella ja täten tutkimustyötä ja materiaalia Blockchainiin liittyen on rajallisesti saatavilla. Suuret tutkimuslaitokset ennustelevat Blockchainin taloudellista läpilyöntiä vuoteen 2025 mennessä.

Tutkimuksen tavoitteena on määritellä Blockchain ja sen toimintaperiaate, tutkia sitä edeltäviä pohjustavia sekä siihen liittyviä teknologioita ja historiaa, tutkia potentiaalisia ja jo käytössä tai prototyyppivaiheessa olevia käyttötapauksia sekä tarkastella teknologian kehityskäyrää. Lisäksi tarkastellaan sitä, kuinka Blockchainia on mahdollisesti hyödynnetty energiateollisuudessa, eritoten Suomalaisessa energiayritys Fortumissa.

Menetelmäsuuntauksena toimii laadullinen tutkimus. Tutkimusmetodologiana käytetään monitapaustutkimusta, jonka lisäksi menetelmänä on exploratiivinen tutkimus jo olemassa olevan materiaalin voimin. Ajankohtaiset artikkelit, uutiset, kirjateokset, tutkimuslaitosten laatimien tutkimusten tulokset ja vastaava materiaali tukevat tutkimusta.

Tutkimuksen tulokset viittaavat siihen, että Blockchain mahdollistaa monia eri toteutuksia eri aloilla, erityisesti energiateollisuudessa ja Fortumin kaltaisen yrityksen tapauksessa. Käyttötapauksia ja onnistuneita pilotointeja on useampia. Tutkimus selkeyttää ja tarjoaa dataa muun muassa taloudellisten, lainopillisten, sosiaalisten sekä teknologisten kehityskeinojen rakentamiseen. Blockchain on selvästi monia mahdollisuuksia avaava teknologia, joka on kuitenkin vielä tutkimusvaiheessa.

Asiasanat
Blockchain, lohkoketju, tietosuoja, vertaisverkko, tietoturva, kryptografia, hajauttaminen, tietokanta, internet, kryptografia, teollinen internet, tietoverkot, energiateollisuus

Sisällysluettelo

Terminologia

Blockchain	Julkinen, kryptografialla suojattu hajautettu digitaalinen lokikirja, joka perustuu vertaisverkkoteknologiaan
Kryptovaluutta	Digitaalisessa muodossa oleva valuuttayksikkö, tai voimavara. Usein toteutetaan Blockchain-tekniikalla
Vertaisverkko / P2P	Internetin verkko, jossa keskitetyn palvelimen tai asiakkaan sijasta verkkoon liitetyt käyttäjät tukevat verkostoa
Hajauttaminen	Transaktiot ja tapahtumat toteutuvat ilman kolmannen osapuolen tahon väliintuloa, käyttäen vahvaa kryptografiaa. Millään yksittäisellä taholla ei ole valtaa transaktioiden hallintaan ilman konsensusta
Solmu/Node	Erilaisia tehtäviä suorittava Solmu tietoverkossa, muun muassa validoinnin konsensuksen varmistamiksesi
Konsensus	Tietoverkon solmujen välillä vallitseva yhteisymmärrys
IoT	Internetin fyysisten objektien verkosto, joka sisältää integroitua teknologiaa, joka mahdollistaa laitteiden välisen kommunikaation
Hash	Satunnaisesta merkkijonosta koostuva yksilöllinen kryptografinen tiiviste
SHA-256	Moderni hajautusalgoritmi, joka toimii nykypäivän standardina. Kooltaan 256 bittiä.

1 Johdanto

Johdantokappaleessa esitellään tutkimuksen motivaatio, aihe, tutkimustavoitteet, metodologia eli käytetyt tekniikat ja menetelmät, tutkintokysymykset, sekä opinnäytetyön rakenne.

1.1 Tausta

Blockchain on termi, jota on usein käytetty kryptovaluuttojen, erityisesti Bitcoinin-nimisen kryptovaluutan asiayhteydessä. Vuoden 2017 loppupuolella Bitcoin koki suuren hintapiikin ja täten aihe sai jalansijaa niin valtavirtamediassa kuin tavallisten ihmisen keskuudessakin.

Käsitteenä se ei kuitenkaan ole uusi. Bitcoin on ollut olemassa jo vuodesta 2008. Tuolloin Satoshi Nakamoto -niminen henkilö tai salanimi julkaisi 1. marraskuuta 2008 oman tutkimuspaperinsa nimeltään "Bitcoin: A Peer-to-Peer Electronic Cash System", liittyen Bitcoiniin ja sitä ylläpitävään Blockchain-teknologiaan.

Tutkimuksessaan (2008) Nakamoto ilmoitti maailmalle, että digitaalinen kaupankäynti Internetissä on tullut tilanteeseen, jossa kolmannen osapuolen finanssialan instituutiot käsittelevät maksutapahtumia yksinoikeudella. Vaikka järjestelmä oli monilta osin onnistunut ja transaktiot yleisesti olivat onnistuneita, kärsi se luontaisesta viasta. Tämä näennäinen luottamus kolmansiin osapuoliin tapahtumien varmistajana paljasti ongelmia luottamuspohjaisessa mallissa. Korkeiden palvelumaksujen lisäksi osa tapahtumista epäonnistui ja tietty prosentuaalinen määrä tapahtumista oli jo tuomittu epäonnistumaan tietoturvaaukkojen ja huijauksien takia. Järjestelmä kärsi tietynlaisesta luottamuspulasta, ja täten tapahtuneiden liiketapahtumien peruuttaminen oli lähes mahdotonta.

Nakamoto (2008) esittää paperissaan ratkaisua ongelmalle kertomalla, että puhtaasti vertaisverkkoon perustuva elektroninen käteinen sallisi kaupankäynnin yhdeltä osapuolelta toiselle ilman finanssialan instituution väliintuloa. Digitaaliset allekirjoitukset ovat osana ratkaisua. Pääasialliset hyödyt kuitenkin menetetään, mikäli kaksoisveloituksen (double-

spending, digitaalisen valuutan mahdollinen virhetilanne, jossa sama digitaalinen valuutta veloitetaan kahdesti) torjumiseksi vaaditaan edelleen kolmas osapuoli varmentajaksi. Kaksoisveloitus-ongelmaan tarjotaan vertaisverkoston (Peer-to-Peer, p2p) käyttämistä. Verkosto aikaleimaa (timestamp) tapahtumat osaksi ketjua käyttämällä hajautusalgoritmia (hashing) ja liittää ne osaksi hash-algoritmiin perustuvaa Proof-of-Work –menetelmää. Proof-of-Work –protokollaa tarvitaan lohkon lopullista validointia varten. Verkosto luo tällä rekisterin, jota ei voi muuttaa ilman, että Proof-of-Work –menetelmä tarvitsee tehdä uudestaan. (Nakamoto, 2008.)

Blockchain konseptina on tärkeä siksi, että sillä voidaan luoda korkean tason tietoturvallisuutta ja läpinäkyvyyttä transaktioissa käyttäen vahvaa kryptografiaa. Blockchain toimii myös p2p-vertaisverkkojärjestelmässä, joten tapahtumat hyväksytään lokikirjaan konsensuksen muodossa. P2p:llä viitataan hajautettuun vertaisverkkoon, jossa keskitettyä auktoriteettia ei ole. Kaikki tietoverkon solmut ovat yhteydessä jokaiseen muuhun solmuun ja omaavat samat oikeudet. Tämä toimii Blockchainin valttikorttina verrattuna keskitettyihin järjestelmiin, ja täten tekee siitä mielenkiintoisen kilpailevan teknologian.

Nasdaqin (2017) artikkelin mukaan Blockchain-teknologiaa käyttävät yritykset ovat saaneet miljardeja dollareja rahoituspääomaa ja useampi Fortune 500 –yritys etsii nyt perinteisille ongelmille ratkaisuja Blockchainin hajautetun tietokannan kautta. Blockchainista puhutaan teknologiapiireissä enemmän kuin koskaan aikaisemmin. Mutta yleinen kysymys on seuraavanlainen: Mikä tekee Blockchainista huomion kiinnittämisen arvoisen?

McKinsey Global Instituten (2013) tuottaman tutkimuksen mukaan 12 suurta nousevaa teknologiaa tulevat muuttamaan elämäämme, taloutta ja liiketoiminnan mallia. Näihin teknologioihin kuuluvat muun muassa Internet of Things, pilvipalvelut, robotiikka, autonomiset ajoneuvot yms. McKinsey on tullut keräämiensä tietojen pohjalta johtopäätökseen, että näillä teknologioilla voi potentiaalisesti olla 14-33 triljoonan dollarin suuruinen taloudellinen vaikutus vuoteen 2025 mennessä.

Tutkimuksen pääasiallisena motivaationa on henkilökohtainen kiinnostus aihetta kohtaan. Alkuperäinen idea tutkimuksen aluille panoon on eräs vaihto-opiskeluvuoden takainen kurssi, jossa käsiteltiin kryptovaluuttoja ja niitten vaikutusta valuuttamarkkinoihin. Kuitenkaan kiinnostukseni ei päättynyt kryptovaluuttoihin, vaan jatkui ja kohdistui pääasiallisesti tämän virtuaalivaluutan takana olevaan teknologiaan, Blockchainiin eli lohkoketjuteknologiaan. Tämän kurssin opettaja huomasi kiinnostukseni ja suositteli kirjoittamaan opinnäytetyötä pelkän kryptovaluutan sijaan Blockchainista, hyvin idealistisesti, mutta samalla objektiivisesti kertoen teknologian suuresta potentiaalista tulevaisuuden eri aloille.

1.2 Tutkimustavoitteet ja tutkimuksen alue

Tämän tutkimuksen tavoitteena on selvittää, onko Blockchainin tuomia potentiaalisia hyötyjä mahdollista hyödyntää energiateollisuudessa, etenkin Fortumin kaltaisen yrityksen tapauksessa. Tutkimuksessa käydään läpi Blockchainin teoriaa, teknisiä ominaisuuksia, toimintaperiaatetta, tietoperustaa ja sitä millaisia taloudellista, lainopillista, sekä teknologista merkitystä kyseisellä teknologialla on tänä päivänä. Tämän lisäksi käydään läpi Blockchainin historiaa sekä edeltäviä vastaavanlaisia ja/tai Blockchainille pohjaa luovia teknologioita. Tämän jälkeen käydään läpi jo olemassa olevia ajankohtaisia sekä lähitulevaisuuden potentiaalisia käyttötapauksia eri teollisuuden aloilta. Empiirisen osuuden viimeisenä osana käydään läpi Blockchain-teknologian merkitystä ja mahdollisia käyttötapauksia Suomalaisissa energiateollisuuden yrityksissä, kuten Fortumissa. Lopuksi käydään läpi tutkimustulokset.

Tutkimus pyritään rajaamaan siinä määrin, että aihe on hyvin laaja eikä täten jokaista käyttötapausta voida sisällyttää tähän tutkimukseen. Tutkimuksessa käydään läpi Blockchainin toimintaperiaatteita, määritellään Blockchain konseptina, käydään läpi teoriaa, sekä tietoperustaa. Teoriaosuus jakautuu yleiseen teoriaan, sekä tutkimuskontekstiin liittyvään, opinnäytetyön tutkimusongelmaan liittyvään spesifiin teoriaan. Tutkimus sisältää haastattelun Suomalaiselta Blockchainia käyttävältä energia-alan yritykseltä, ja tämän haastattelun löydöksiä käydään läpi analyysiosiossa.

Mainittakoon kuitenkin, että vaikka tämä tutkimus ei suoranaisesti tutki Bitcoinia tai kryptovaluuttoja ja niiden vaikutusta yhteiskunnassa ja elektronisessa kaupankäynnissä, on aihe silti erittäin relevantti Blockchainin toimintaperiaatteen ymmärtämiseksi. Toisin sanoen Blockchainin käyttötapauksia on useampia ja kryptovaluutta on yksi niistä. Sitä voitaisiin tietyllä tavalla kutsua modernin Blockchain-teknologian pioneeriksi.

Kyseessä on laadullisin menetelmin suoritettava tutkimus. Sen yhtenä rajoitteena on epäkypsä tiedon laatu, sillä määrällistä aineistoa ei kovin paljoa ole ja empiirinen tutkimus on täten suoritettava laadullisen tutkimuksen puitteissa. Tutkimus pyrkii käymään aihetta läpi mahdollisimman objektiiviselta kannalta ja antamaan tai viittaamaan kaikille väittämille selkeitä perusteluja.

1.3 Tutkimuskysymykset

Tutkimuskysymyksillä tarkoitetaan sitä, mihin avainkysymyksiin tutkimus hakee vastauksia ja lisää ymmärrystä verrattuna nykytietoon. Teorian tehtävä on luoda teoreettinen tieto-

pohja asetettuihin tutkimuskysymyksiin. Lisäksi teoria tarjoaa käsitteistön, jolla voidaan operoida tutkimusdataa valitun metadatan puitteissa.

Päätutkimuskysymyksenä ja tavoitteena kuitenkin löytää selkeyttä seuraavaan:

1. Edellyttäen, että Blockchainia voidaan hyödyntää energiateollisuudessa, millaisia käyttötapauksia tämä mahdollistaa Fortumin tapauksessa? Millä tavalla hyödyt ilmenevät käytännössä, ja millaiset käyttötapaukset olisivat höydyllisiä Fortumille?

1.4 Metodologia

Tutkimusmetodologia viittaa käytettyihin tutkimusmenetelmiin ja tutkimuksen tiedonkeruun lähestymistapoihin. Tässä työssä tutkimusmetodologiana käytetään Multiple Case Studya, eli monitapaustutkimusta. Yleisesti ottaen tapaustutkimuksessa viitataan sellaiseen tutkimukseen, jossa tutkitaan yhtä tiettyä ajankohtaista ilmiötä ja sen käytännön kontekstia perusteellisesti. Monitapaustutkimuksella viitataan sellaiseen tutkimukseen, joka rakentuu kahden tai useamman tapauksen ympärille. (Yin, 2014)

Monitapaustutkimusten perusteella kerätty aineisto ja johtopäätökset ovat usein laadukkaampia ja herättävät enemmän kiinnostusta. Tämän ansiosta tutkimus nähdään usein kokonaisuutena vahvempana ja vakaampana kuin tapaustutkimus (Single Case Study). (Yin, 2014)

Aiheen metodologiaa rajoittaa kuitenkin jo edellä mainittu tiedon puute ja aiheen suhteellinen tuoreus. Tämän vuoksi monitapaustutkimuksen lisäksi lähestymistapana käytetään eksploratiivista lähestymistapaa. Tällä menetelmällä pyritään tekemään tutkimusta uudesta, etsivästä näkökulmasta. Eksploratiivisella tutkimuksella pyritään selvittämään tutkimuskysymyksiä, jättäen tilaa mahdolliselle jatkotutkimukselle. Tutkimuksen tarkoituksena ei ole vielä antaa vakuuttavaa näyttöä ja johtopäätöksiä, vaan se auttaa meitä ymmärtämään paremmin ilmiötä ja ongelmaa. (Dudovskiy, 2019)

Kyseistä tutkimusmenetelmää käytetään myös, mikäli tutkimusaihe on vielä uusi ja mahdollisesti vähän tunnettu. Vaikkakin Blockchain on tietyllä tapaa tuttu konsepti varsinkin tietotekniikan ja digitaalisen liiketoiminnan maailmassa, on se kuitenkin vielä valtavirtaväestölle melko uusi konsepti. Aihe saattaa nousta usein vaikkapa kryptovaluuttoihin liittyvässä keskustelussa, kuitenkin usein puutteellisella ymmärryksellä.

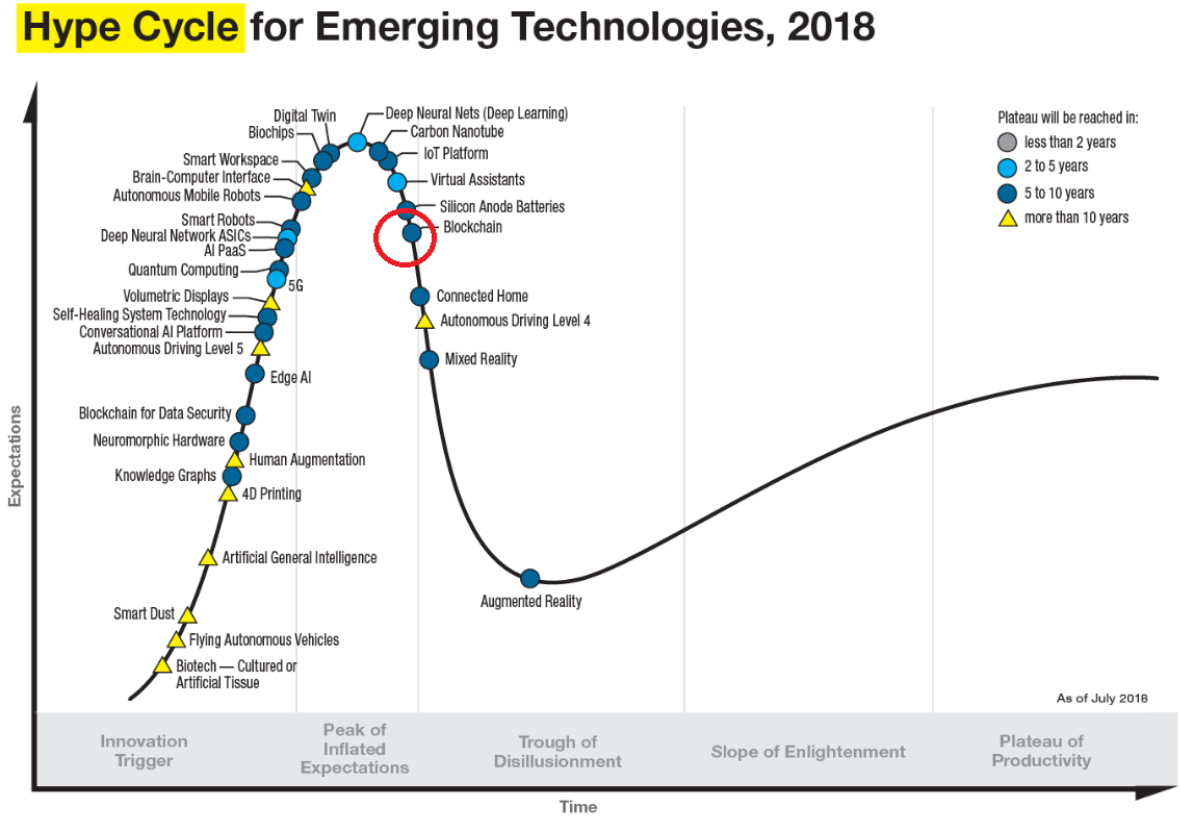
Tiedonhankintamenetelmiin kuuluu kirjateokset, erilaiset artikkelit, akateemiset julkaisut, Google Scholarin tieteelliset tutkimukset, tunnettujen tieteen ja teknologian tutkimuslaitosten tuottamat tutkimustulokset, Haaga-Helia ammattikorkeakoulun virtuaalinen lähdemateriaali sisältäen e-kirjat, tieteelliset tutkimukset ja muu vastaava aineisto. Tämän lisäksi Tiedonhankintaan käytetään haastattelua suuren Suomalaisen sähkö- ja energiayhtiön R&D (tutkimus ja kehitys) -osaston vastaavalta, avaten tärkeitä käyttötapauksia sähkö- ja energianjakelun alalta. Tällä saadaan tuotua selkeästi esiin Blockchainin maailmaa asiantuntijan näkökulmasta.

2 Tietoperusta

Tietoperusta-osio on jaoteltu kahteen osa-alueeseen; Yleiseen tietoperustaan sekä niin sanottuun käsiteanalyysiin, eli tutkimuskontekstiin liittyvään teoriaan. Käsiteanalyysilla luodaan käsitteistö teoriaan, joka on sidoksissa Blockchainin tutkimuskontekstiin ja sitä ympäröivään käsitteistöön.

Tietoperusta-osiossa puhutaan Blockchainista konseptina ja käydään läpi sen perimmäistä toimintamallia. Kappaleessa esitellään lisäksi perusteellisesti muuta olennaista teknistä tietoa, kuten esimerkiksi verkkoympäristön toimintaa, eri tietoverkkojen muotoja, tietorakenteita, tietoturva-protokollia, sekä lohkon teknistä sisältöä. Tämän lisäksi käydään läpi historiaa ja edeltäviä relevantteja konsepteja ja teknologioita, esimerkiksi Byzantine Fault Tolerancea. Tämän jälkeen esitellään argumentteja toimintamallin puolesta sekä perustellaan sitä, mihin ongelmaan Blockchain oletetusti tuo ratkaisua. Lopuksi esitellään Blockchainien eri muodot.

Blockchainin päämääräinen valtti piilee siinä, että se luo hajautettua yhteisymmärrystä (konsensusta) tuottavan järjestelmän digitaalisessa verkkomaailmassa. Tämä sallii osaaottavien kokonaisuuksien olemaan ajan tasalla siitä, että digitaalisesti varmistettu ja kiistämätön tapahtuma on luotu ja kirjoitettu tietokantaan muistiin. (Crosby, Pattanayak, Verma, Kalyanaraman, 2016.)



Kuva 1. Kehittyvien teknologioiden suosion mittari. Blockchain korostettuna punaisella. (Gartner, 2018)

Kehittyvät teknologiat yleisesti ottaen vaativat tukea uusista teknisistä perusteista ja uusista dynaamisista ekosysteemeistä. Nämä ekosysteemit tarvitsevat tuekseen uusia liiketoimintastrategioita ja siirtyvät alustapohjaisiin liiketoimintamalleihin. (Gartner, 2018.)

Gartnerin (2018) tekemän tutkimuksen mukaan Blockchain voisi olla todellinen suuri muutoksen tekijä, sillä se omaa todellista potentiaalia keskitettyjen järjestelmien luotettavuuden ja läpinäkyvyyden lisäämiseen.

2.1 Yleinen teoriaosuus, The Byzantine Generals Problem

Nasdaqin artikkelin (2017) mukaan ominaisuus, jota kutsutaan nimellä ”Byzantine Fault Tolerance” (BFT), on ymmärtämisen arvoinen käsite, mikäli haluaa saada kaiken irti Blockchainin mahdollisuuksista. Tietokoneiden kyky hallita ja torjua ”Byzantine failures” -tyyppisiä vikatilanteita on olennainen osa Blockchainin kykyä ylläpitää luotettavia tapahtumalokikirjoja läpinäkyvästi ja peukaloinnilta suojatulla tavalla. (Nasdaq 2017.)

Liiketoiminnan tietojenkäsittelyn alkuvaiheessa 1980-luvun alkupuolella tiedemiehet ja insinöörit alkoivat tutkia tietokoneiden luotettavuutta. Yhteisymmärryksellä oli päätetty, että luotettava tietotekninen järjestelmä on oltava kykeneväinen selviytymään yhden tai

useamman järjestelmän komponentin vikatilasta. (Bambara & Allen, 2017.) Tämän tyyppisestä tilanteesta selviytymiseen on esitetty Lamportin, Robert Shostakin, ja Marsall Peasen vuonna 1982 julkaisemassa paperissa *Byzantine Generals Problem*, josta ongelman nimikin juontaa juurensa. Tätä abstraktia ongelmaa ja sen ratkaisuja täten käytetään luotettavien Blockchainien täyttöön panossa.

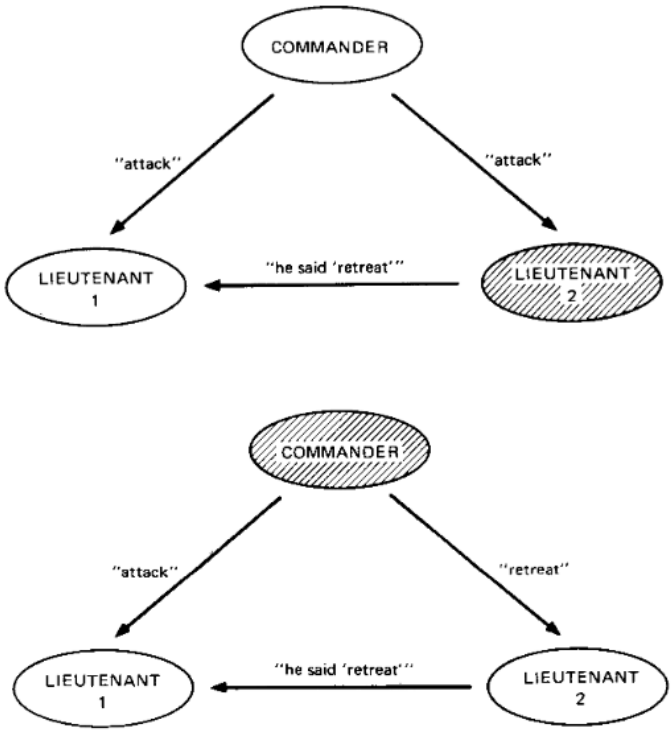
Eräs tapa ymmärtää Blockchainia on katsoa sitä kolmen tunnetun tieteenalan yhteenottona; peliteorian, kryptografian, sekä tietotekniikan fuusiona. Nämä tieteenhaarat ovat olleet olemassa jo pitkään, mutta ensimmäistä kertaa kohtaavat nyt sopusoinnussa ja luovat pohjan Blockchain-teknologialle. (Mougayar 2016.)

Peliteoria tutkii ”älykkäiden rationaalisien päätöksentekijöiden konfliktin ja yhteistyön matemaattista mallia”. Tämä käsite on määritelty taloustieteilijä Roger B. Myersonin teoksessa *Game theory: analysis of conflict.* (1997). Tämä määritelmä liittyy Blockchainiin siinä määrin, että suunnitellessaan Bitcoinin ja Blockchainin konseptia Satoshi Nakamoto kohtasi tunnetun peliteorian arvoituksen nimeltään ”*The Byzantine Generals Problem*” (BGP).

BGP on tunnettu analogia matemaatikkojen ja tietojenkäsittelijöiden maailmassa. Lamport, Robert Shostak, ja Marsall Pease (1982) hahmottelivat skenaarion, jonka mukaan joukko Bysantin armeijaa johtavia kenraaleja piirittävät kaupunkia ja pyrkivät luomaan hyökkäysstrategiaa. Yksinkertaisimmillaan, kenraalit voivat päättää joko hyökätä tai perääntyä. Toiset kenraalit päättävät hyökätä, kun taas osa perääntyä. On huomioitava, että jokainen kenraali hyväksyy yhteisen päätöksen, sillä vain muutaman kenraalin koordinoima hyökkäys olisi innoton, sekasortoinen, ja huonompi vaihtoehto kuin koordinoitu hyökkäys tai perääntyminen. Pulmaa monimutkaistaa petturien läsnäolo, jotka eivät vain voi äänestää epäoptimaalista strategiaa, vaan he voivat tehdä niin omavaltaisesti.

Esimerkkinä seuraava tilanne; yhdeksän kenraalia päättää äänestää hyökkäyksestä. Neljä kenraalia on hyökkäystä vastaan ja neljä puolella. Täten yhdeksäs kenraali voi lähettää äänestyksen vetäytymisestä perääntymisen puolella oleville kenraaleille, ja hyökkäyksen puolella olevan äänen muille. Ne, jotka vastaanottavat perääntymiskäskyn tältä yhdeksänneltä kenraalilta, perääntyvät, kun taas loput hyökkäävät (mikä ei välttämättä tuota haluttua lopputulosta hyökkääjille). Ongelma monimutkaistuu siinä määrin, että kenraalit ovat fyysisesti erotettuja. Täten he joutuvat lähettämään äänensä kuriirien voimin, jotka taas voivat epäonnistua tehtävässään tai väärentää ääniä. (Lamport, Shostak & Pease, 1982.)

Pähkinänkuoressa, kyseinen analogia perustuu siihen kuinka komentava kenraali päättää hyökätä tai perääntyä, ja miten hän välittää tämän päätöksen muille kenraaleille. Osa on pettureita mukaan lukien potentiaalisesti kenraali itse. Pettureihin ei voi luottaa viestin välityksessä, ja mikä pahempi, he voivat muokata viestin sisältöä, muuttaen prosessia. (Bambara, Allen, 2017.)



Kuva 2. Byzantine Generals Problem kaavion muodossa (Lamport, Shostak, Pease, 1982)

Ylemmässä kuviossa toinen kenraali (lieutenant) on petturi. Alemmassa sen sijaan komentaja on petturi. Tämän analogian mukaan kenraalit nähdään kollektiivisesti prosesseina. Ylimmän käskyn aloittava kenraali on prosessin lähde ja muille prosesseille lähetetyt käskyt ovat viestejä. Petturit ja alemmat (lieutenant) kenraalit ovat viallisia prosesseja ja uskolliset kenraalit ja alemmat kenraalit ovat oikeita prosesseja. Hyökkäys tai perääntyminen viestitetään yhden ainoan bitin muodossa: yksi (1) tai nolla (0). (Bambara, Allen, 2017.)

Yhteysymmärryksen ongelman ratkaisun saavuttamiseen on läpäistävä kolme koetta tai vaatimusta: päättäminen (termination), yksimielisyys (agreement) sekä oikeellisuus (validity). (Bambara, Allen, 2017.) Kun näitä periaatteita sovelletaan BGP:ssä, näyttävät ne seuraavalta:

1. Ratkaisun on taattava, että kaikki oikeat prosessit päättävät lopulta niiden antamien käskyjen arvosta

2. Kaikkien oikeiden prosessien tulee päättää annetulle käskylle samanlainen arvo

3. Mikäli alkuperäinen lähdeprosessi on oikea prosessi, tulee kaikkien prosessien päättää alkuperäinen prosessin antama arvo
   (Bambara, Allen, 2017.)

Tunnetusti paras tapa käyttöönottaa luotettavaa ja varmaa tietojärjestelmää (tässä tapauksessa Blockchainia) on käyttää useita eri suorittimia saman tuloksen laskelmointiin. Tämän jälkeen voidaan suorittaa enemmistöpäätös, jonka tuotoksista lasketaan yksittäinen arvo. (Bambara, Allen, 2017.)

Alla taulukossa on kuvailtuna Blockchainin ja BGP:n haasteet rinnakkain.

Kenraalit		**Blockchain**
Sopu Strategiasta	Tavoite	Sopu pätevistä transaktioista
Erotetut leirit	Jakelu	Jaetut solmut (nodes) tietoverkossa
Uskolliset joukot ja kenraalit	Hyvät	Todenperäiset solmut
Petturit	Pahat	Pahat (corrupt) solmut
Viestin vääristys	Hyökkäys	Lisää epäkelvon transaktion Blockchainiin
Mistä tietää mikä viesti on tosi	Ongelma	Mistä tietää, mikä transaktio on aito
Ei ole	Ratkaisu	Proof-of-Work
Ei ole	Konsensus	Vaikeampi Blockchainin toteutus

Taulukko 1. BGP:n ja Blockchainin haasteet rinnakkaisena analogiana (Bambara & Allen, 2017)

Nykypäivänä Byzantine Fault Tolerance on käytössä monessa eri yhteydessä. Yhtenä esimerkkinä mainittakoon Bitcoin. Bitcoin-verkosto toimii rinnakkain Proof-of-Work –protokollan avulla. Suoriutuakseen Byzantine –tyyppisistä vikatiloista ja saavuttamaan

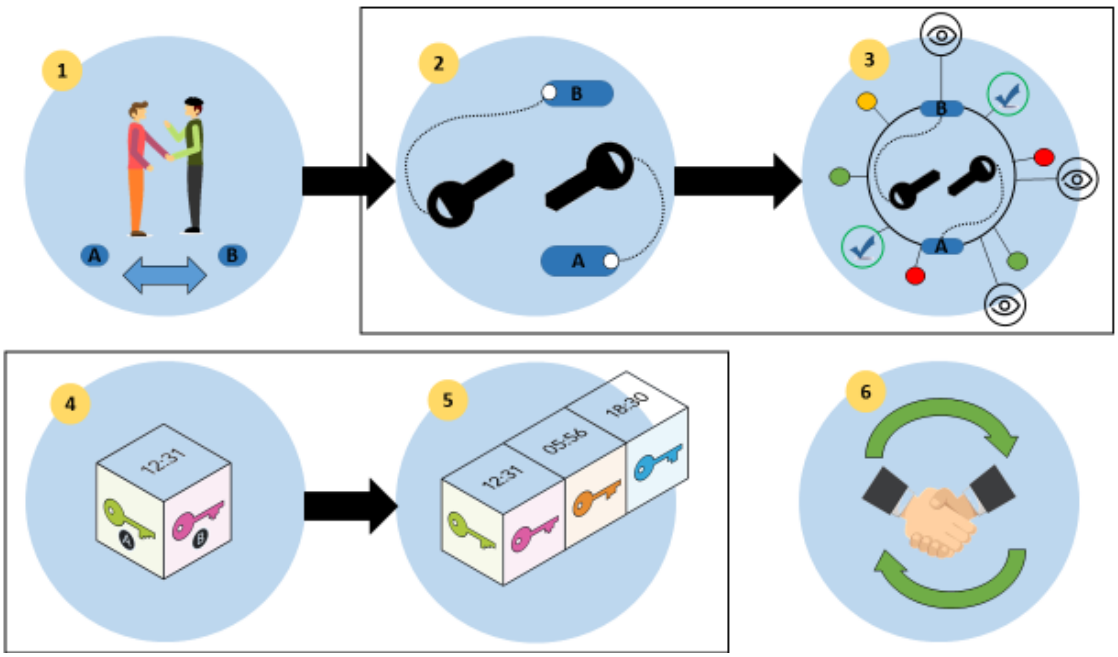
johdonmukaisen kokonaisnäkemyksen järjestelmän tilasta, on Proof of Work- ketju on avaintekijänä. (Bambara, Allen, 2017.)

Monet ilma-alusjärjestelmät, kuten Boeing 777 ja 787:n erilaiset turvajärjestelmät käyttävät Byzantine Fault Tolerancea hyödykseen. Nämä ovat kuitenkin reaaliaikaisia järjestelmiä, joten ratkaisuiden tulee olla käytännössä viiveettömiä (low latency). Esimerkiksi Boeing 777:n Safebus-tietoverkkojärjestelmä voi saavuttaa BFT:n alle mikrosekunnin viiveellä. (Bambara, Allen, 2017.)

Jotkut avaruusalukset, kuten SpaceX:n, Dragon flight system ottavat huomioon Byzantine Fault Tolerancen jo suunnitteluvaiheessa sisäänrakennettuna järjestelmään. BFT-mekanismit käyttävät komponentteja, jotka toistavat saapuvan viestin (tai vain sen nimikirjoituksen) muille kyseisen saapuvan viestin vastaanottajille. Nämä kaikki mekanismit olettavat, että viestin toistamisen tapahtuma estää Byzantine-oireiden etenemisen. Järjestelmät, joissa on korkean tason turvallisuus tai vikakriittisyys, nämä olettamukset on todistettava tosiksi hyväksyttävän tason vikasietokattavuudella. Kun välitetään todistetta testaamisen keinoin, eräs hankaluus on luoda riittävän kattavia signaaleja Byzantine-oireilla. Tämänkaltaiset testausmetodit vaativat mitä luultavammin erikoistunutta vianhakujärjestelmää. (Bambara, Allen, 2017.)

2.1.1 Toimintamalli

Liiketapahtumat voidaan validoida ja vahvistaa ilman kolmannen osapuolen välttämätöntä väliintuloa. Seuraava kuva demonstroi julkisen Blockchainin liiketapahtumaketjua flowchart-kaaviona.



Kuva 3. Julkisen Blockchainin liiketapahtuma flowchart-kaaviona (Bambara J; Allen P, 2017)

Blockchainit ovat avoimia ja hajautettuja tietokantoja, jotka kykenevät dokumentoimaan kahden osapuolen välisiä tapahtumia tehokkaasti. Tähän käytettävä menetelmä on varmennettavissa ja pysyvä, kuten esitettynä ylläolevassa kaaviossa. (Kuva 3.)

Kuvassa kolme on esiteltynä yksinkertaistettu Blockchainilla toteutettu kuusivaiheinen liiketapahtuma. Siinä kaksi osapuolta haluaa suorittaa transaktion Blockchainin kautta. Kaksi osapuolta haluaa suorittaa liiketapahtuman. Tässä tapauksessa henkilöt A ja B haluavat suorittaa liiketapahtuman käyttäen Blockchain-protokollaa. Transaktio laitetaan alulle luomalla RSA-avainpari molemmille osapuolille. Avainpari on osana digitaalisen allekirjoituksen protokollaa sisältäen julkisen sekä yksityisen avaimen. Tässä vaiheessa kummallakin osapuolella on hallussaan yksityinen sekä julkinen avain. Näitä avaimia käytetään datan allekirjoittamiseen, salaamiseen, sekä purkamiseen. (Bambara, Allen, 2017.)

Tämän jälkeen hajautetun tietoverkon osanottajat eli solmut (nodes) todistavat liiketapahtuman todeksi käyttäen Proof-of-Work –protokollaa. Tätä protokollaa käytetään konsensuksen ja varmenteen luomiseen hajautetussa tietoverkossa. Kun tapahtuma on varmennettu, luodaan seuraavaksi uusi lohko. Jokainen lohko sisältää tietyt attribuutit. Lohko lisätään lohkoketjun jatkumoksi ja ketjutetaan toisiinsa peruuttamattomasti kiinni käyttäen hajautusfunktiota (hash-tiiviste). Tämän toteuduttua liiketapahtuma on suoritettu ja sen tiedot säilötty pysyvästi Blockchainiin. (Bambara, Allen, 2017.)

1. Osapuolet A ja B haluavat suorittaa liikevaihdon
2. Molempien osapuolien haltuun luovutetaan tapahtuman turvaamiseksi kryptografiset avaimet (RSA keys, julkinen ja yksityinen avain)
3. Hajautettu tietoverkosto todistaa ja varmistaa tapahtuman
4. Tapahtuman varmistuttua, uusi Block (lohko sisältäen määrätyt attribuutit) luodaan
5. Tämän jälkeen lohko lisätään ketjun jatkumoksi
6. A:n ja B:n välinen liiketapahtuma on suoritettu

Varmennetut lohkot ovat suunniteltu vastustamaan muutoksien tekemistä. Toisin sanoen, lohkon dataa ei voi muuttaa takautuvasti. Käyttäen hajautettua verkostoa (P2P) ja aikaleimapalvelinta (timestamp server) julkisen Blockchainin tietokanta kykenee ylläpitämään itse itseään autonomisesti. Tietokanta voidaan myös ohjelmoida siten, että tapahtumat voidaan käynnistää automaattisesti. (Bambara, Allen, 2017.)

Tyypillisesti täysi auktoriteetti johonkin asiaan on säännöstelty käyttäjänimien ja salasanojen kautta. Julkinen blockchain kuitenkin käyttää näiden sijasta kryptografiaa. (Bambara, Allen, 2017.)

William Mougyar ja Vitalik Buterin kertovat teoksessaan ”The Business Blockchain” (2016), että Blockchainin käsite voidaan katsoa monen eri näkökulman kautta. Määritelmät voidaan kuitenkin pääpiirteittäin jakaa kolmeen ryhmään:

Tekniset määritelmät; back-end tietokanta, joka ylläpitää hajautettua lokikirjaa avoimesti ja tietoturvallisesti

Liiketaloudelliset määritelmät; varallisuuden siirtämisestä vertaisverkostossa (Peer-to-Peer, P2P)

Lainopilliset määritelmät; järjestelmä transaktioiden validointiin ilman kolmannen osapuolen välikäden avuntarvetta

Blockchainin toiminnallisuus = tekniset + liiketaloudelliset + lainopilliset määritelmät. (Mougyar, Buterin, 2016.)

2.1.2 Tietorakenne

Tässä osioissa käsitellään Blockchainin tapahtumien lokikirjan teknistä rakennetta ja yleisiä ominaisuuksia. Teoriaosio käy jokaisen vaiheen läpi pääpiirteittäin teknisestä näkökulmasta.

Bambara ja Allen (2017) kertovat, että yksinkertaisimmillaan Blockchain on hajautettu tietokanta kattaen fyysisen ketjun kiinteän pituisia lohkoja, sisältäen vähintään 1 tai N määrän tapahtumia. Näissä ketjuissa jokainen lohkoon lisättävä tapahtuma varmennetaan (validation) ja lisätään lohkoon. Lohkon valmistuttua lisätään uusi lohko jo olemassa olevan lohkoketjun jatkumoksi. Siinä missä klassinen CRUD (Create, Read, Update, Delete) sisältää useamman mahdollisen toiminnan, sisältää Blockchain vain kaksi; ”add transaction” (lisää tapahtuma) sekä ”view transaction” (katsele tapahtumaa).

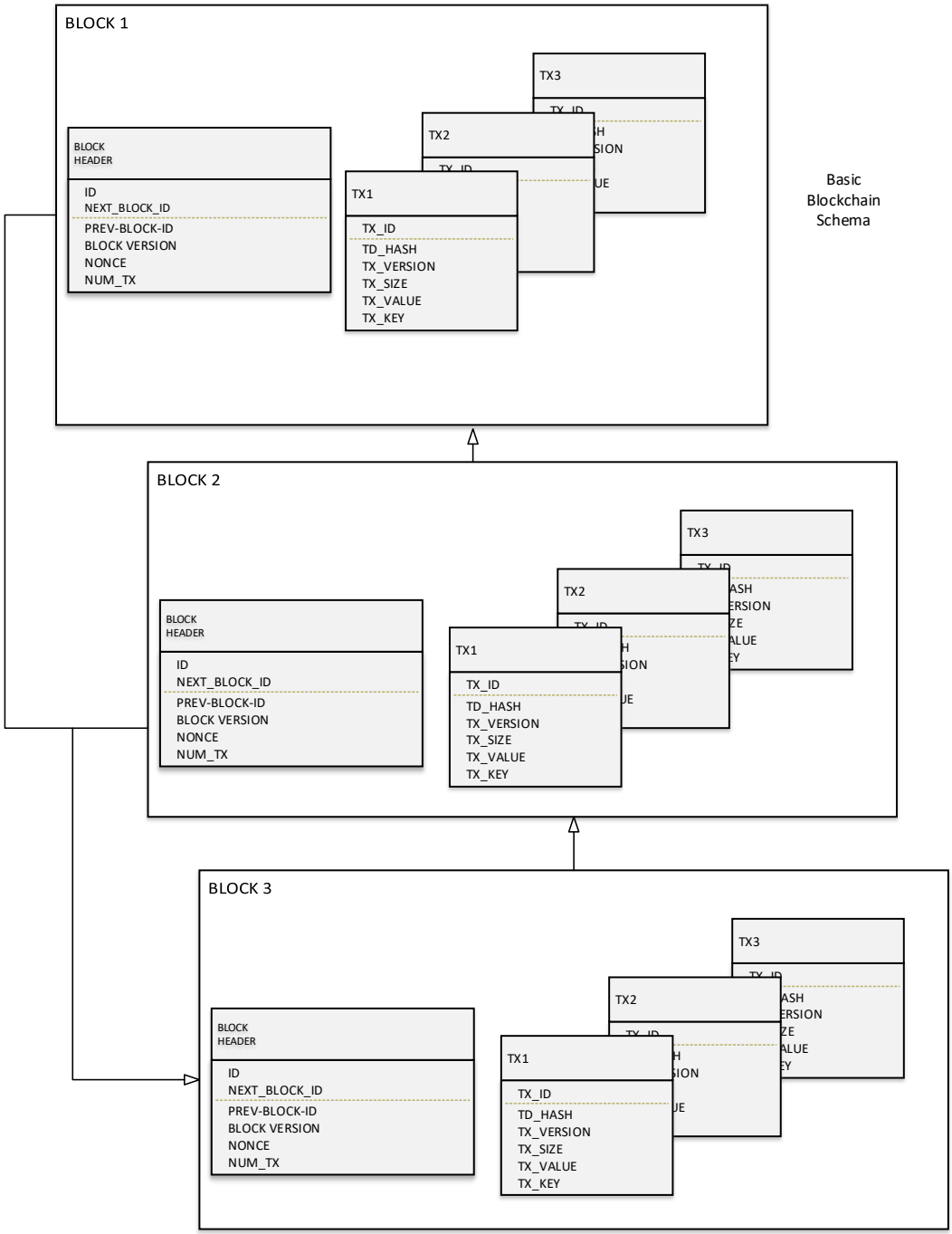
Bambara ja Allen (2017) kuvailevat kolme toiminnallista peruselementtiä seuraavasti:

- Uuden ja hävittämättömissä olevan tiedon lisääminen ja ”lohkoiksi” järjestäminen

- Jokaisen tapahtuman varmentaminen lohkoissa kryptografialla
- Uuden lohkon lisääminen jo olemassa olevan ja muuttamattoman lohkoketjun jatkumoksi

Jokainen uusi luotu lohko on ”ketjutettu” edelliseen lisättyyn Blockchainin lohkoon ja säilyttää sen digitaalista sormenjälkeä.

Alla Blockchainin datakaavio relaatiotietokannan muodossa.



Kuva 4. Blockchain data layout (Bambara J; Allen P, 2017)

Kuten yläpuolen kaaviossa esitetään, jokainen Blockchainin lohko sisältää tietyt attribuutit. Lohkon ylätunnus (header, kooltaan noin 200 tavua) sisältää metatietoa, muun muassa edellisen lohkon hash-funktion (SHA-256), aikaleiman ja binääripuu-tietorakenteen. (kuva 4.)

Seuraavaksi käydään läpi lohkon eri attribuutteja. Näissä tavukoot saattavat muuttua. Esimerkkinä Bitcoin-protokollan Blockchain-rakenne:

Block identifier (4 tavua): Blockchain-verkon tunniste. Se sisältää muuttumattoman merkkijonoarvon 0xD9B4BEF9. Tämä merkkijono toimii tunnisteena käytössä olevan datan tai tiedoston tyypille.

Next block identifier (4 tavua): Yllämainittua tunnistetta seuraavan lohkon tunniste.

Block size (4 tavua): Osoittaa sen, kuinka suuri lohko on kooltaan. Alun perin lohkon koko oli kiinteä 1 MB. Tämä tullaan nostamaan tulevaisuudessa kaksinkertaiseksi, kokoon 2 MB. Suurin mahdollinen kapasiteetti on 2GB, joten skaalautuvuustekijä on jo otettu huomioon.

Block version (4 tavua): Jokaisen protokollaa pyörittävän tietoverkon solmun on toteutettava samaa versiota kuin kyseisessä kentässä on mainittu.

Previous Block hash (edellisen lohkon tiiviste, 32 tavua): Tämä on lohkoketjun edellisen (viimeksi lisätyn) lohkon ylätunnuksen digitaalinen tunniste (hash-tiiviste). Se lasketaan keräämällä yhteen ylätunnuksen kaikki osiot (nonce, versio yms.) ja käyttäen kryptografista funktiota (SHA-256) kahdesti järjestämällä uudestaan yksittäisten osioiden tavut.

Block merkle root (tiivistepuu, 64 tavua).

Block timestamp (aikaleima, 8 tavua)

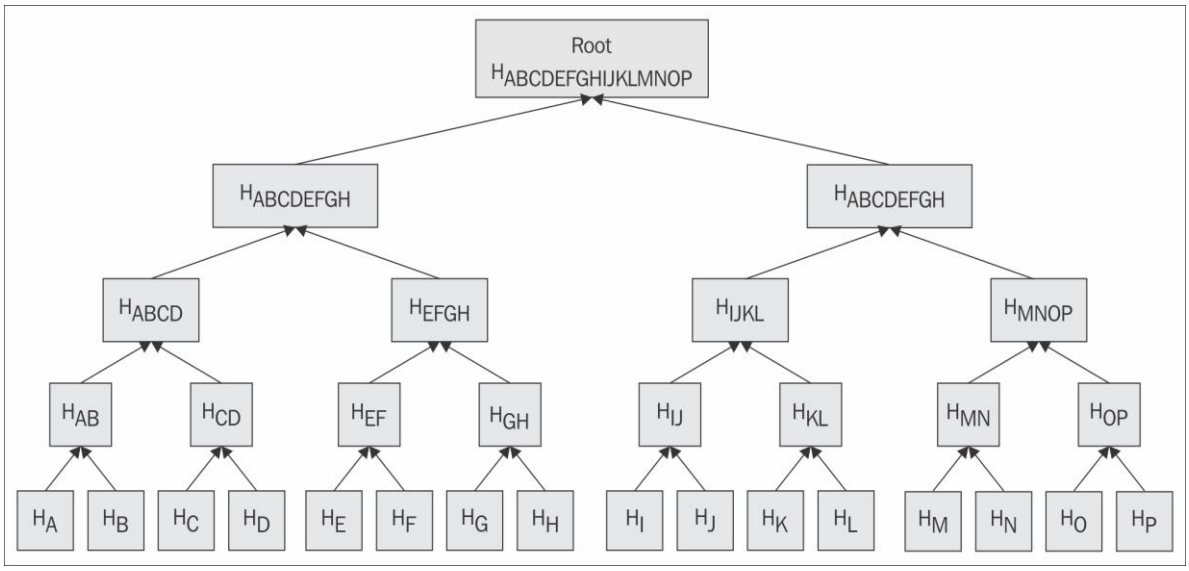
Nonce (satunnainen kertakäyttöinen numero, 4 tavua).

(Bambara, Allen, 2017)

2.1.3 Merkle Tree (Tiivistepuu), SHA-256

Blockchainin eräänä pioneerina voidaan pitää Stuart Haberia ja W. Scott Stornettaa, jotka vuonna 1991 kuvailivat kryptografisesti suojattuja lohkoketjuja. Vuonna 1992 he liittivät malliinsa merkle tree-tietorakenteen eli tiivistepuun, sallien useampien dokumenttien sisällyttämisen lohkoon. (Scott-Biggs, 2018.)

Olennainen osa Blockchainin lohkojen rakennetta on Merkle Treeksi kutsuttu algoritmi. Merkle tree eli tiivistepuu on tärkeä skaalautuvuutta edistävä monitasoinen tietorakenne (binääripuu). Tämä tietorakennetyyppi on erittäin tunnettu ohjelmointikielissä. Merkle treen perimmäisenä tarkoituksena on varmistaa että vertaisverkon välityksellä vastaanotetut tiedostot ovat koskemattomia ja eheitä, ja että niiden alkuperä on jäljitettävissä. (Bambara, Allen, 2017.)



Kuva 5. Merkle Tree-algoritmin rakenne (Bashir, 2017)

Rakenteen juuri (*root*) on ylin solmu. rakenteen alimpia solmuja kutsutaan *leaf* (lehti)-solmuiksi. Jokainen solmu on yksinkertaisimmillaan transaktion kryptografinen hash-tiiviste. Merkle-rakenne ei sisällä listaa tapahtuneista transaktioista. Sen sijaan se säilyttää pelkän hash-tiivisteen kaikista tapahtumista yllä kuvatun puun kaltaisen tietoranteen tavoin. (Kuva 5.)

Haber ja Stornetta pohtivat sitä, miten digitaalisia tiedostoja pursuavassa maailmassa dokumenttien muokkaushistoria voidaan varmistaa pitäen samalla niiden sisältö salattuna. Ratkaisuksi Haber ja Stornetta toteuttivat dokumenttien tiivisteistä (sekalaisen merkkijonon synnyttämä yksilöllinen tunniste) muodostettavan ketjun, joka jaetaan satunnaisille käyttäjille aikaleimattavaksi. (Hallamaa, 2018.)

Hallamaa (2018) kertoo Blockchainista ja tiivistepuusta analogian muodossa. Ryhmä laboratoriotutkijoita tekee joka päivän päätteeksi tiivisteen muistiinpanoistaan. Jokainen tutkija kirjoittaa jokaisen rivin alkukirjaimen tai numeron peräkkäin paperille. Päivän lopuksi paperit kootaan yhteen, jonka jälkeen jokainen yhdessä hyväksyy paperien sisällön. Lopuksi satunnaiset ryhmän jäsenet leimaavat tiivisteet ja ne laitetaan laboratorion seinälle vierekkäin. Täten kukaan ei voi jälkeen päin muuttaa omia muistiinpanojaan, sillä ne eivät enää täsmäisi jo seinällä olevien tiivisteiden kanssa. (Hallamaa, 2018.)

Kuitenkin haasteeksi tulee vastaan seinätilan puute. Tähän perustuu Haberin ja Stornettan lisäämä tiivistepuu eli hash tree. Tiivistepuu mahdollistaa tiivisteiden kokoamisen yhteen uudeksi tiivisteeksi. Tällä kertaa tutkijoiden tiivisteet laitetaan laatikkoon, joka leimataan ja laitetaan hyllylle edellisen laatikon viereen. Jokainen laatikko viittaa edelliseen laatikkoon muodostaen ketjun, jonka järjestystä ei voi muuttaa. (Hallamaa, 2018.)

2.1.4 Hyödyt, haasteet ja riskit

Seuraava kysymys on se, että mitä hyötyä hajauttamisesta on ensi sijassa? Millä tavalla keskitetty järjestelmä eroaa hajautetusta järjestelmästä? Buterinin (2017) mukaan yleisimmät argumentit hajauttamisen puolesta ovat seuraavat:

- Vikasietokyky (*Fault Tolerance*) — hajautetut järjestelmät vikaantuvat epätodennäköisemmin, sillä ne tukeutuvat moniin erilaisiin komponentteihin, jotka eivät ole samankaltaisia toisiinsa nähden

- Hyökkäyksenesto (*Attack resistance*) — hajautettuihin järjestelmiin on kalliimpi hyökätä, tuhota tai manipuloida, sillä niissä ei ole arkaluonteisia yksittäisiä vikaantumispisteitä (central point of failure) joihin on mahdollista hyökätä kustannustehokkaammin kuin ympäröivään järjestelmään

- Väärinkäytön esto (*Collusion resistance*) — Hajautettuihin järjestelmiin osaa ottavien on vaikeampi harrastaa vilpillisiä toimintatapoja niin, että hyödyt kerätään muiden osanottajien kustannuksella
  (Buterin, 2017.)

Kuten missä tahansa uudessa nousevassa ja kasvavassa teknologiassa, on myös Blockchainissa omat haasteensa. Blockchain tarjoaa luotettavuutta hajautetun tietoverkon keinoin. Blockchainin avulla parannetaan turvallisuuden jäljitettävyyttä, tietojen ja tapah-

tumien avoimuutta osallistujille ja säätelijöille, sekä alhaisempia toimintakustannuksia. Älykkään sopimuksen yhdistäminen Blockchainiin tarjoaa varmuutta, turvallisuutta ja kestävyyttä. Lisäksi Blockchainiin säilötty data on suojattu tietoturvauhilta, sillä tietoverkkoa ylläpitää useampi solmu (node). Teoriassa yli 51 prosenttia solmuista tulisi olla vaarannettuja ennen kuin mitään ongelmia ilmenisi. (Bambara, Allen, 2017.)

Avainhaasteet Bambaran ja Allenin (2017) mukaan ovat seuraavia:

Suorituskyky. Tapahtumien käsittelyyn, validointiin ja petosten havaitsemiseen vaadittavat laskentaresurssit ja suorituskyky määrittelevät sen, mihin pankki-, rahoitus- ja maksupalveluihin niitä voidaan parhaiten soveltaa. Tällä hetkellä Blockchain ei ole riittävän tehokas käsittelemään tuhansia tapahtumia sekunnissa. Sitä käytetään useimmiten varainsiirroksiin, jotka eivät ole riippuvaisia ajasta, toisin kuin esimerkiksi epävakaiden arvopaperien osto ja myynti.

Yhteistoimivuus. Yhteensopivuuden varmistaminen erilaisten Blockchainien välillä, jotta ne voivat kommunikoida keskenään. Mikä on tämän saavuttamisen hinta?
Tämä määräytyy sidosryhmien mukaan, jotka tulevat toivottavasti kehittävään tiettyjä standardeja.

Skaalautuvuus. Jokaisen Blockchain-verkoston solmun tulee tietää jokaisesta maailmanlaajuisesta tapahtumasta. Tämä voi aiheuttaa merkittävää tietoverkon hidastumista. Tavoitteena on kyetä suorittamaan joka tapahtuma korkealla tehokkuudella, kuitenkaan uhraamatta hajautetun tietoverkon tarjoamaa tietoturvaa.
(Bambara, Allen, 2017.)

Toimiakseen oikein Blockchain vaatii standardisoituja sääntöjä, jonka mukaan jokainen osanottaja menettelee. Näin varmistaan järjestelmän virheettömyys ja luotettavuus. Hajautettu malli muodostaa haasteita siinä vaiheessa, kun sääntöjä pitää muuttaa. Tämä johtuu siitä, että säännöt tulee yksimielisesti hyväksyttää osallistujien toimiakseen erheettömästi. (Bambara, Allen, 2017.)

2.2 Blockchainin tietoperusta

Kappaleessa 2.1 käsiteltiin Blockchainiin liittyvää teoriaa yleisellä tasolla. Kappaleessa 2.2 käydään läpi olennaisia tutkimuskontekstiin eli Blockchain-teknologiaan liittyviä käsitteitä. Käsiteanalyysillä viitataan teoriaan, jolla luodaan käsitteistö Blockchainin tutkimuskontekstille.

Johdannossa mainitaan kuinka Blockchain tunnettiin alun perin ja usein vieläkin Bitcoinin asiayhteydessä. Kun ajan myötä ihmiset alkoivat ymmärtää Blockchainin toimintaperiaatteita, alkoivat käyttötapaukset myös lisääntyä; arvokkaan tiedon säilöminen tietokantaan, henkilöllisyys, sopimukset, omistusoikeudet ja moni muu. (Bambara, Allen, 2017.)

2.2.1 Blockchainien eri muodot

Blockchainin eri kategoriat ovat lisääntyneet. On olemassa niin sanottuja julkisia Blockchaineja, joita jokainen voi katsella ja päivittää, sekä yksityisiä Blockchaineja rajoitetulle ryhmälle, esimerkiksi yhtiön tai organisaation jäsenille. Tämän lisäksi on vielä kolmas muoto eli konsortiomuotoiset Blockchainit, joita käytetään yhteistyössä muiden yritysten kanssa. Tämä jälkimmäisin muoto on yleinen esimerkiksi Wall Streetin maailmassa, jossa viisi suurinta sijoituspankkia ovat tietynlaisessa sopimuksessa keskenään. Myös energiateollisuudessa on usein eri yritysten välisiä konsortioita yhteisten tavoitteiden saavuttamiseksi. (Bambara, Allen, 2017.)

Seuraavaksi tutkitaan eri muotoja hieman yksityiskohtaisemmin.

Julkinen Blockchain (*Public Blockchain*) on yleisin kolmesta muodosta. Julkinen Blockchain on juuri se versio, josta alkuperäiset kehittäjät usein puhuivatkin; kaikille julkisesti saatavilla oleva Blockchain. Hajautettu lokikirja, jossa tapahtumat voidaan sisällyttää vain ja ainoastaan jos ne ovat päteviä. Julkisessa Blockchainissa kaikki osanottajat voivat kollektiivisesti olla mukana luomassa konsensusta. (Bambara, Allen, 2017.) Konsensusprosessi määrittelee sen, mitkä lohkot lisätään ketjun jatkumoksi ja mikä senhetkinen tila on. Julkisen Blockchainin turvaamiseen käytetään keskuspalvelimen sijasta kryptografiaan perustuvia menetelmiä, joita tuetaan louhijoiden (miners) palkkioilla. Koska julkisessa Blockchainissa kukaan yksittäinen käyttäjä ei ole valtuutettu varmentamaan tapahtumia, kaikki käyttäjät noudattavat tietynlaista algoritmia ja protokollaa. Tämä varmentaa tapahtumat käyttäen ohjelmiston ja laitteiston resursseja ratkaisemaan ongelmaa väsytyshyökkäyksen (brute force) keinoin (toisin sanoen ratkaisemalla kryptografinen ongelma). Louhija, joka ratkaisee ongelman ensimmäisenä, palkitaan. Jokainen ratkaisu mukaan lukien tapahtumat, joita käytettiin varmistamaan niitä, luovat pohjan seuraaville ratkaistaville ongelmille. Nämä varmennusmenetelmät ovat *Proof-of-Work ja Proof-of-Stake.* (Bambara, Allen, 2017.)

Konsortio-Blockchain (Consortium Blockchain) on osittain yksityinen hajautettu lokikirja, jossa konsensusprosessia ohjaa muutama ennalta valikoitu tietoverkon solmu. Esimerkki-

nä yhdeksän rahoitusalan instituution yhteenliittymä, joista jokainen käyttää solmua ja joista viiden (esimerkiksi Yhdysvaltain korkein oikeus) tulee vahvistaa jokainen lohko ennen sen hyväksyttämistä. Tämän kaltaiset Blockchainit ovat hajautettuja lokikirjoja, joita voidaan nähdä ”osittain hajautettuina”. (Bambara, Allen, 2017.)

Yksityinen Blockchain (Private Blockchain) on Blockchainin muoto, jossa digitaaliset kirjoitusoikeudet ovat keskitetysti yhden organisaation hallussa. Lukuoikeudet voivat olla omavaltaisesti julkiset tai rajoitetut. Todennäköisiin sovelluksiin voi sisältyä yksittäisen yritysten tietokantojen hallinta sekä sisäinen tarkastus, joten julkinen luettavuus ei ole välttämätöntä monissa tapauksissa. Kuitenkin joissain tapauksissa julkinen tarkasteltavuus on haluttua. (Bambara, Allen, 2017.)

Yksityiset Blockchainit voisivat tarjota ratkaisuja taloudellisiin haasteisiin, sisältäen sisäisen valvonnan toimijoiden (compliance agents) sisällyttämisen tunnettuihin säännöksiin. Näihin säännöksiin kuuluvat muun muassa Health Insurance Portability and Accountability Act (HIPAA, 1996), anti-money laundering (AML) sekä know-your-customer (KYC) -lait. (Bambara, Allen, 2017.)

Nämä kolme mainittua Blockchainin muotoa on tärkeää erottaa toisistaan. Yksityisessä Blockchainissa on julkiseen verrattuna monia etuja. Yksityisessä Blockchainissa toimija voi muuttaa Blockchainin sääntöjä. Mikäli kyseessä on liiketoimintakumppanien välinen Blockchain, on helpompi korjata liiketapahtumien mahdollisia vikatilanteita. Myös saldoja voidaan muokata ja ylipäätään mitä tahansa kumota. Siitä huolimatta on olemassa polku, joka johtaa tapahtumien alkuperään. Yksityisen Blockchainin liiketapahtumat ovat edullisempia toteuttaa, sillä korkean tason suoritustehoa saavuttamiseksi vaaditaan vain muutaman luotetun solmun varmennus. Vaikka esimerkiksi Ethereumin tuoma proof-of-stake –algoritmi tuo julkista Blockchainin lähemmäksi ihanteellista ”välitöntä vahvistusta”, on yksityinen Blockchain aina nopeampi. Tähän syynä se, että valitettavasti valonnopeus ei kaksinkertaistu joka kahden vuoden välein kuten Mooren laissa (transistorimäärän kaksinkertaistuminen mikropiireissä kahden vuoden välein). (Bambara, Allen, 2017.)

Lisäksi kun puhutaan konsensusalgoritmeista, tulee harkita "permissioning" -menetelmää. Tämä määrittelee sen, kuka saa hallita ja osallistua konsensusprosessiin. Kolme suosittua menetelmää ovat:

- Julkinen (Proof-of-Work, Proof-of-Stake yms.)
- Yksityinen (salattuja avaimia käytetään luomaan valtuutusta rajattuun Blockchainiin)

- Semi-yksityinen (Muun muassa konsortiopohjaiset, perinteinen Byzantine Fault Tolerance käytössä liittoutuneella tavalla)
  (Mougyar, Buterin, 2016.)

Edellä mainitut seikat vahvistavat argumenttia, jonka mukaan yksityiset Blockchainit ovat optimaalisia instituutioiden käyttöön. Kuitenkin julkisilla Blockchaineilla on myös paljon arvoa instituutioiden asiayhteydessä. Tämä arvo piilee filosofisissa hyveissä, joista julkisen Blockchainin kannattajat ovat usein puhuneet. Näitä arvoja ovat muun muassa vapaus, neutraliteetti ja avoimuus. (Bambara, Allen, 2017.)

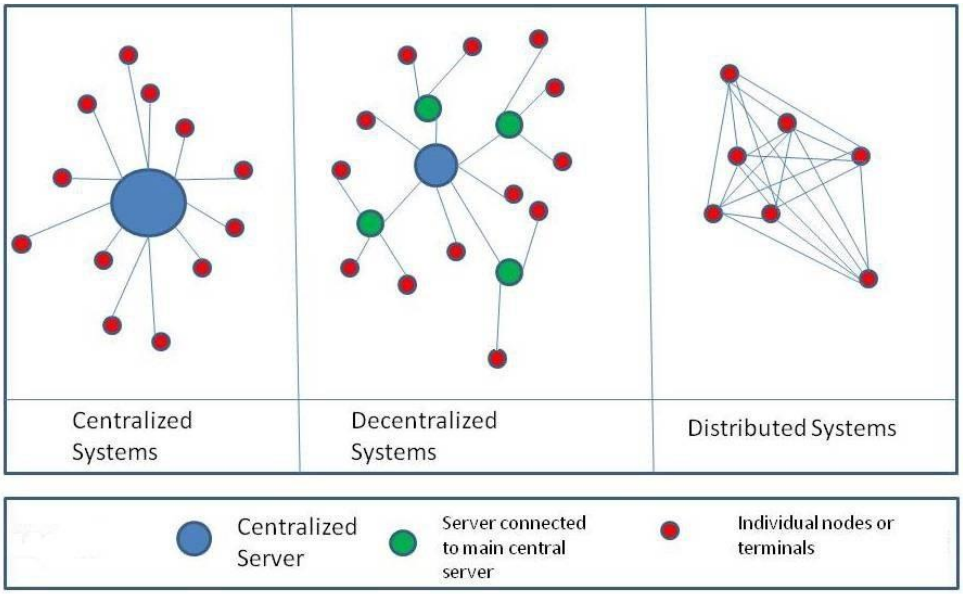
Julkisen Blockchainin hyödyt jakautuvat pääsääntöisesti kahteen kategoriaan:

- Julkiset Blockchainit takaavat sovellusten loppukäyttäjille suojaa kehittäjiltä vakiinnuttaen sen, että edes kehittäjillä ole valtuuksia tehdä tiettyjä modifikaatioita

- Julkiset Blockchainit ovat avoimia ja täten monen entiteetin käytössä. Tällä on vaikutus liikesuhteiden solmintaan. Mikäli Blockchainissa on varallisuutta säilyttäviä järjestelmiä ja valuuttajärjestelmä samassa Blockchainissa, voidaan kustannukset tiputtaa lähelle nollaa käyttämällä älykkäitä sopimuksia (smart contract). A voi lähettää varallisuutta sovellukselle, joka taas lähettää sen osapuolelle B hetkessä. B lähettää sovellukselle rahat, sillä ohjelma toimii julkisella Blockchainilla ja on täten luotettava. On kuitenkin huomioitava, että toimiakseen tulee kahden täysin heterogeenisen eri toimialan varallisuusluokan (asset class) olla samassa tietokannassa. Myös muut varallisuuden haltijat, muun muassa kiinteistörekisterit, voivat käyttää tätä järjestelmää.
  (Bambara, Allen, 2017.)

2.2.2 Tietoverkot ja hajautettu verkkoympäristö

Blockchainin ja Bitcoinin maailmassa usein kuulee puhetta hajauttamisesta (Decentralization) ja hajautetuista tietoverkoista (Decentralized networks). Valitettavasti näistä on usein muodostunut iskusanoja ilman vankkaa ymmärrystä tietoverkkojen rakenteiden eroista. Käsitteitä ei pystytä usein erottelemaan johdonmukaisesti toisistaan ja määritelmät saattavat olla monitulkintaisia.



Kuva 6. Tietoverkkojen eri muodot (Vaidya K, 2016)

Yllä oleva kaavio esittää keskitetyn, keskittämättömän, sekä hajautetun tietoverkkojärjestelmän erot. Sininen edustaa keskitettyä palvelinta, kun taas vihreä edustaa pääpalvelimeen yhdistettyä palvelinta. Punainen edustaa yksittäisiä päätteitä tai tietoverkon solmuja. (Kuva 6.)

- **Keskitetyissä järjestelmissä** (*Centralized Systems)* on olemassa yksi keskeinen auktoriteetti tai palvelin. Muut tietoverkon solmut toimivat tietoverkon asiakkaina tai yksilöinä, hyväksyvät vastaanottamansa viestin ja toimivat sen mukaisesti.
- **Hajautetuissa järjestelmissä** (*Decentralized Systems*) on olemassa useampi palvelin, joka vastaanottaa viestejä yhdeltä pääpalvelimelta. Yksittäiset tietoverkon solmut ovat yhteydessä toissijaisiin palvelimiin. Kuitenkin joissain järjestelmissä kaikki palvelimet voivat olla hierarkkisesti tasavertaisia ilman keskitettyä palvelinta.
- **Vertaisverkkojärjestelmissä** (*Distributed Systems, Peer-to-Peer*) keskitettyä auktoriteettia ei ole. Kaikki tietoverkon solmut ovat yhteydessä jokaiseen muuhun solmuun ja kaikilla solmuilla on samat oikeudet ja auktoriteetti. Kun puhutaan tietoteknisistä hajautetuista järjestelmistä, jokaisen tietoverkon solmun prosessointiteho voi vaihdella laaja-alaisesti.

(Vaidya K, 2016.)

Vitalik Buterin kirjoittaa Mediumin artikkelissaan (2017) että kun puhutaan ohjelmistojen hajauttamisesta, saatetaan itse asiassa puhua kolmesta erilaisesta hajauttamisen osa-alueesta. Joissain tapauksissa voi olla vaativaa määritellä sitä, miten toinen voi olla mah-

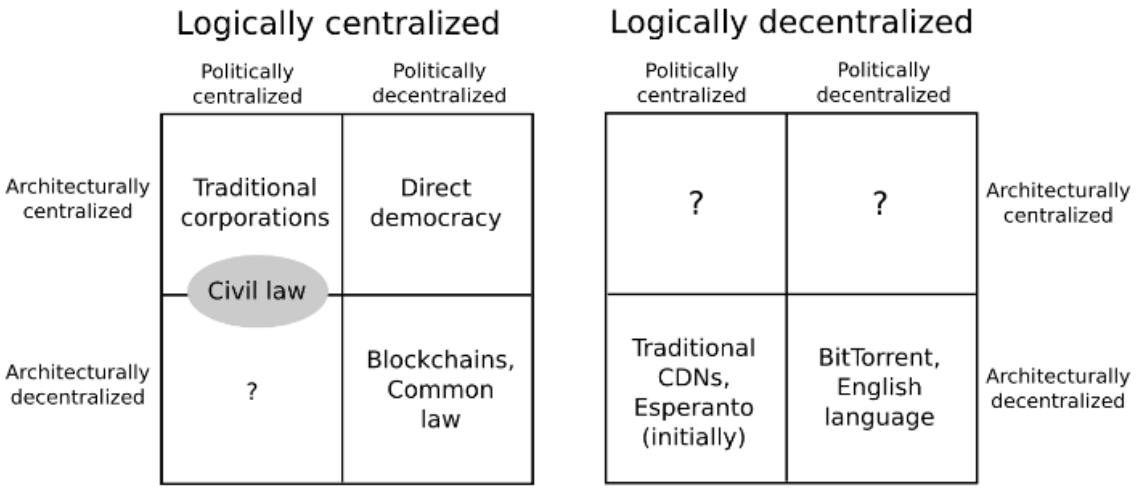
dollista ilman toista. Tosiasiassa ne ovat kuitenkin jokseenkin riippuvaisia toisistaan. Buterin määrittelee nämä osa-alueet seuraavasti:

Arkkitehtuurillinen hajauttaminen—monestako fyysisestä tietokoneesta järjestelmä muodostuu? Kuinka monen tietokoneen vikatilannetta järjestelmä pystyy vastustamaan minä hetkenä hyvänsä?

Poliittinen Hajauttaminen—kuinka monta yksilöä tai organisaatiota viime kädessä kontrolloi tietokoneita, joista järjestelmä muodostuu?

Looginen hajauttaminen—näyttääkö järjestelmän ylläpitämä ja esille tuoma käyttöliittymä ja tietorakenteet yhdeltä yhtenäiseltä kokonaisuudelta vai epämääräiseltä joukolta? Eräs heuristiikka voisi olla se, että jos järjestelmä puolitetaan sisältäen palveluntarjoajat sekä käyttäjät, kykeneekö kumpikin osapuoli jatkamaan toimintaansa itsenäisesti ja yhtenäisenä?

Nämä kolme osa-aluetta voidaan pyrkiä lokeroimaan alla olevan kaavion mukaan:



Kuva 7. Keskitetyn ja hajautetun järjestelmän nelikenttäkaavio (Buterin, 2017)

Buterin (2017) tarkentaa artikkelissaan kuinka yllä mainittu kaavio on kuitenkin karkea ja avoin tulkinnalle. Artikkelissa käydään kaavion sisältöä läpi seuraavasti:

- Perinteiset korporaatiot ovat poliittisesti keskitettyjä (yksi toimitusjohtaja), arkkitehtuurillisesti keskitettyjä (yksi pääkonttori) sekä loogisesti keskitettyjä (ei voida puolittaa)

- Siviililainsäädäntö (Civil law) tukeutuu keskitettyyn lainsäädäntöelimeen, kun taas yleinen lainsäädäntö perustuu yksittäisistä tuomareista koostuviin ennakkotapauksiin. Siviililaissa on kuitenkin joitain piirteitä arkkitehtuurillisesta hajauttamisesta, sillä monilla tuomioistuimilla on suuri harkintavalta, muttei kuitenkaan yhtä paljon kuin yleisellä lainsäätöelimellä. Kuitenkin kumpikin voidaan määritellä loogisesti keskitetyksi (”Laki on laki”).

- Kielet voidaan määritellä loogisesti hajautetuksi. Esimerkiksi Alicen ja Bobin välillä englanniksi käymä keskustelu, sekä Charlien ja Davidin välinen keskustelu eivät ole velvoitettuja olemaan yhteydessä toisiinsa. Kieliin ei ole olemassa keskitettyä infrastruktuuria eikä englanninkielisen kieliopin sääntöjä luoda tai valvota yhdenkään yksittäisen henkilön toimesta (kun taas esperanto oli alun perin Ludwig Zamenhofin luoma, tosin nykyään se toimii enemmänkin kielenä joka kehittyy vähitellen ilman auktoriteettia)

- BitTorrent on englannin kielen tavoin loogisesti hajautettu. Sisällönjakeluverkot (CDN) ovat samankaltaisia, mutta silti yhden yhtiön kontrolloimia.

- Blockchainit ovat poliittisesti (ei valvovaa auktoriteettia) sekä arkkitehtuurina hajautettuja (ei infrastruktuurillista keskinäistä vikaantumispistettä), mutta toisaalta loogisesti keskitettyjä (on yksi yleisesti sovittu tila ja järjestelmä toimii ja käyttäytyy kuin yksi tietokone)
  (Buterin, 2017.)

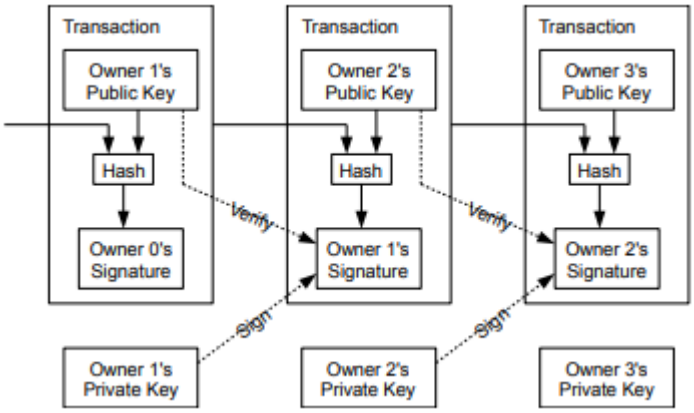
2.2.3 Kryptografia

Tässä kappaleessa esitellään kolme tärkeää Blockchainin käyttämää suojausmenetelmää sekä perustellaan sitä, että mikä on niiden tärkeys Blockchainin kannalta.

Blockchainin toimintamalli suojataan ja validoidaan kolmella olennaisella menetelmällä. Nämä menetelmät ovat; digitaaliset allekirjoitukset, Hash-algoritmit, sekä esimerkiksi Proof-of-Work -menetelmän kaltaiset konsensusprotokollat.

Hash-algoritmi on kryptografiaan perustuva hajautusfunktio. Se on matemaattinen algoritmi, joka kuvaa satunnaisen kokoista dataa ja muuntaa sen kiinteäksi määrätyn kokoiseksi Hash-tiivisteeksi. Syöte (input) voi olla lyhyt tai pitkä, mutta tulostus on aina kiinteän kokoinen merkkijono. Se on suunniteltu yksisuuntaiseksi operaatioksi eikä sitä voida enää peruuttaa. (Jscrambler, 2017.)

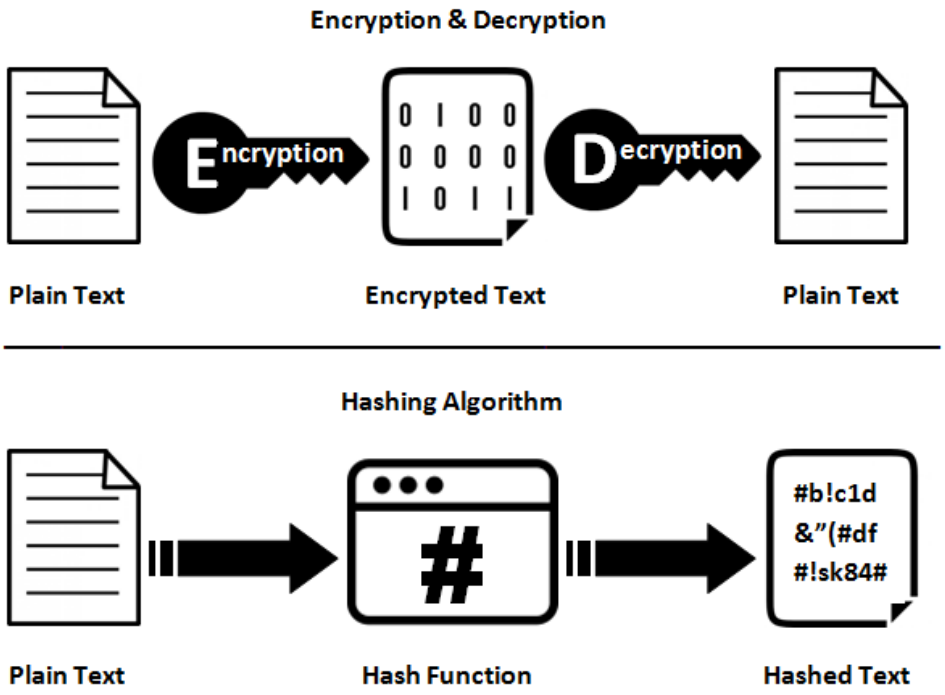
Hash-funktioita on useita erilaisia, esimerkiksi MD-5 sekä SHA-256. Blockchainin Hash-funktiona käytetään SHA-256 –protokollaa. SHA tulee sanoista Secure Hash Algorithm, ja sitä käytetään tiedon eheyden varmistamiseksi. Samasta syötteestä (input) tuotetaan aina sama tuloste (output). Tämä tuloste tulee aina olemaan kooltaan 256 bittiä tai 32 tavua syötön koosta riippumatta. Mikä tahansa pienikin muutos syötössä muuttaa tulosteen. Samasta syötteestä ei voida saavuttaa useampia tulosteita. Kuitenkin tulosteesta ei koskaan voida päätellä syöttöä. Tämä tekee SHA-256 –algoritmista erittäin tietoturvallisen. (Bambara, Allen, 2017.)



Kuva 8. Blockchainin liiketapahtumien kryptografinen toimintakaavio (Nakamoto, 2008)

Asianomaisille jaetaan RSA-Avainpari. Tämä avainpari sisältää yksityisen (private) sekä julkisen (public) avaimen. Yksityistä RSA-avainta käytetään digitaalisten allekirjoitusten luomisessa, kun taas julkista RSA-avainta käytetään digitaalisten allekirjoitusten verifioinnissa. (IBM, 2014.) Yllä olevassa kaaviossa kuvataan tätä prosessia. Liiketapahtuman osanottajille jaetaan avainpari, jolla luodaan sekä verifioidaan allekirjoitukset. Tämän lisäksi jokainen lohko sisältää oman hash-tiivisteen sekä edellisen lohkon tiivisteen, luoden ”ketjun”. Nimi ”Blockchain” tai suomeksi ”lohkoketju” on peräisin tästä. (Kuva 8.) Edellisen lohkon hash-arvoa käytetään täten laskemaan nykyisen lohkon hash-arvo luoden yhteyden lohkojen välillä.

Jokaisen lohkon data on täten hash-tiivistetty. Jos lohko muuttuu tavalla tai toisella, esimerkiksi mikäli jokin taho yrittäisi peukaloida lohkon sisältämää dataa tai attribuutteja, muuttuisi lohkon hash-luku. Jokainen tietoverkon solmu huomioi tämän muutoksen. (Au, 2018.)



Kuva 9. Digitaalisen allekirjoitusten ja Hash-funktioiden ero (Nohe, 2018)

Digitaalinen allekirjoitus tapahtuu enkryption eli salauksen kautta. Salaus on kaksisuuntainen funktio, jossa data salataan siten että se voidaan purkaa myöhemmin. Tämä toteutuu edellä mainittujen yksityisten ja julkisten avainten kautta. Hash-funktio on sen sijaan teoriassa yksisuuntainen funktio, jossa data kartoitetaan kiinteän kokoiseksi arvoksi. (Nohe, 2018.)

Konsensus-prosessin tuottamiseksi käytetään Proof-of-Work –protokollaa. Se on konseptiltaan samankaltainen kuin Adam Backin vuonna 1997 kehittämä Hashcash-protokolla. (Nakamoto, 2008.) Hashcashin alkuperäinen idea oli toimia vastakeinona palvelunestohyökkäyksille sekä tämän lisäksi torjua roskapostia ja vastaavia internetin tuomia haitta-elementtejä. (Back, 2002.)

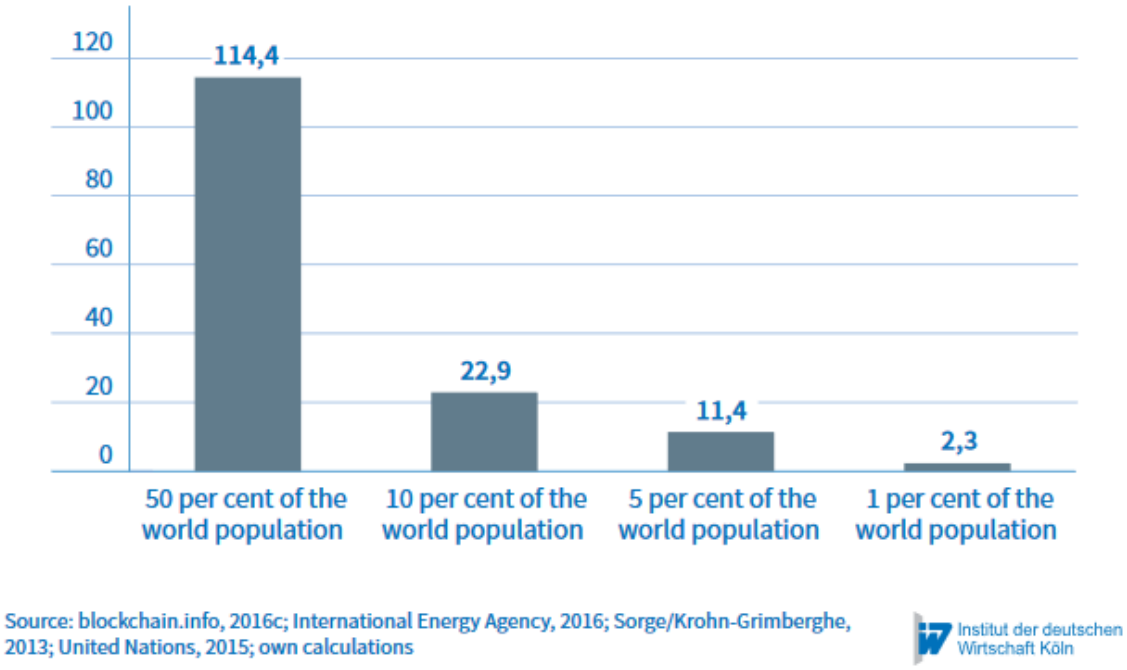
Lyhyesti määriteltynä, tämän kaltaisen konsensusmekanismien tarkoituksena on luoda yhteisymmärrystä – saada meidät luottamaan toisiimme – jotta meidän ei itse tarvitse. (Thake, 2018.)

Proof-of-Work –protokollaa tarvitaan lohkon lopullista validointia varten. Blockchainin tietoverkon osanottajien (solmujen) tulee ratkaista monimutkaisia matemaattisia pulmia ennen kuin lohko voidaan varmistaa eheäksi. Tätä prosessia kutsutaan nimellä louhinnaksi (mining). Osanottajia kutsutaan louhijoiksi (miners). (Thake, 2018.)

Näitä matemaattisia pulmia on hankala laskea mutta helppo verifioida. Kun ongelma on saatu ratkaistua louhijoiden toimesta, palkitaan heidät vastaavalla digitaalisella valuutalla. Tätä tapahtumaa kutsutaan nimellä Block reward (palkkio tehdystä työstä). (Thake, 2018.)

Lohkon tapahtumat täten varmennetaan ja lohko lisätään ketjun jatkumoksi. Tämä vaatii todellista prosessointivoimaa, josta protokollan nimi onkin peräisin. Matemaattisista yhtälöistä tulee joka kerta haastavampia ratkaista. Tätä vaikeustason asteittaista nousua kutsutaan nimellä Block difficulty (lohkon haastavuus) ja se on sisäänrakennettu järjestelmään tarkoituksellisesti. Tarkoituksena on varmistaa, että jokainen louhittu valuutta vaatii huomattavan määrän prosessointitehoa. (Thake, 2018.)

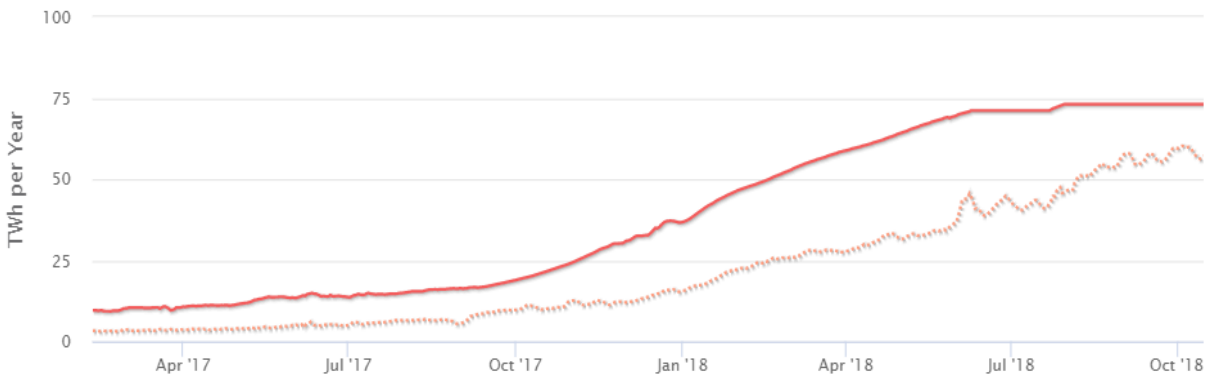
Proof-of-Work –protokolla tarjoaa vaadittua tietoturvaa ja on tähän mennessä todistetusti toiminut hyvin. Se on kuitenkin erittäin paljon energiaa kuluttava prosessi. (Konstantopoulos, 2018)



Kuva 10. Proof-of-Work-tyylisen louhimisprosessin energiankäyttö. (Demary & Demary, 2017)

Joulen alkuvuodesta 2018 tuottaman tutkimuksen mukaan esimerkiksi Bitcoin-verkosto käytti tuolloin keskimäärin 24 terawattituntia energiaa joka vuosi - suurin pirtein yhtä paljon kuin Irlannin valtio. (De Vries, 2018.) Yksittäinen Bitcoin-transaktio vaatii vähintään 300

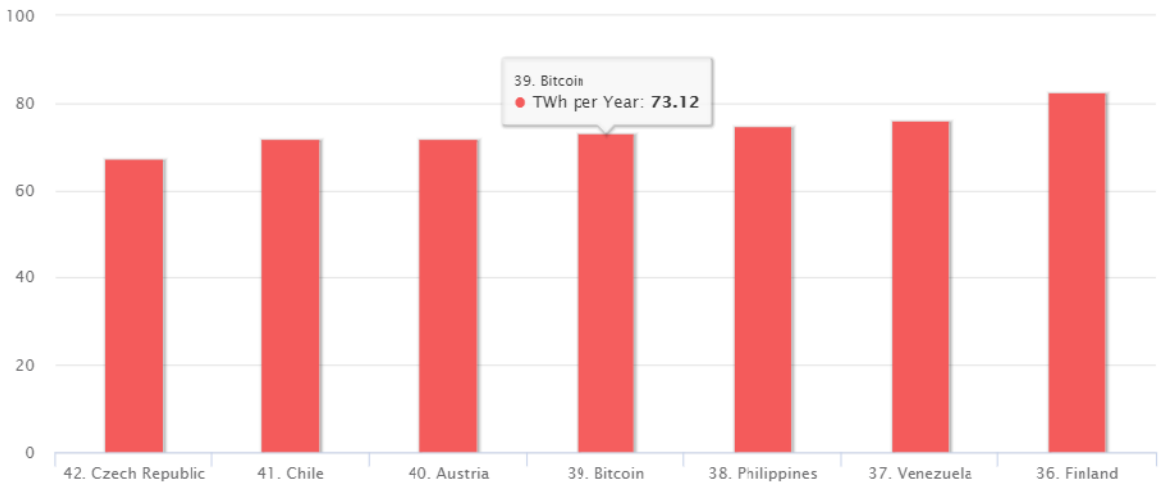
kilowattituntia sähköä, joka on riittävä määrä tyypillisen kodin kuukauden sähkönkulutukseen. (Thake, 2018.)



Kuva 11. Bitcoinin arvioitu keskimääräinen energiakulutus terawattitunneissa. (Digiconomist, 2018)

Yllä olevassa kaaviossa esitellään Bitcoin-verkoston arvoitu vuosittainen energiankulutus aikavälillä 10.2.2017-15.10.2018. Alempi katkoviivalla esitelty käyrä esittää energiankulutuksen vähimmäismäärän terawattitunneissa. Ylempi punainen käyrä esittää arvioidun kokonaisenergiankäytön terawattitunneissa. (Kuva 11.)

Kuten aikaisemmin on jo aikaisemmin mainittu, Bitcoin-verkoston kasvaessa vaaditaan yhä suurempia laskennallisia resursseja. Digiconomistin (2018) laatiman tutkimuksen mukaan energiankulutus tuplaantuu joka kuuden kuukauden välein. Tämän hetkinen (mitattu 15.10.2018) keskimääräinen energiankulutus on 73,12 terawattituntia per vuosi. (Digiconomist, 2018.)



Kuva 12. Bitcoin-verkoston energiankäyttö verrattuna valtioiden kokonaisenergiankäyttöön. (Digiconomist, 2018)

Yllä olevassa kuvassa esitellään sitä, kuinka Bitcoin-verkoston energiankäyttö vertautuu kokonaisten valtioiden energiankäytön kanssa. (Kuva 12) Vasemmassa pylväässä on Tšekin tasavallan vuosittainen energiankäyttö, joka on tällä hetkellä arviolta 63,7 terawattituntia. Suomi on kaavion toisessa päässä ja sen energiankäytön määränä on 82,5 terawattituntia per vuosi. Bitcoin-verkoston energiankäyttö on arviolta 73,12 terawattituntia per vuosi. (Digiconomist, 2018)

Vaikka Proof-of-Work –protokolla on energiaa vaativa ja kallis, on se silti rakenteeltaan suhteellisen turvallinen hyökkäyksiä vastaan. Syynä tähän on se, että yksittäisten tahojen ainoa keino häiritä järjestelmää on hallitsemalla 51% koko verkon laskentatehosta. (Thake, 2018.)

Ennen kaikkea, Proof-of-Work –tyyppinen protokolla varmistaa sen, että Blockchain on pätevä. Se ei kuitenkaan ole äärettömiin skaalautuvissa oleva protokolla. Laitteisto ja energianlähteet ovat loppupeleissä toistaiseksi rajallisia. (Thake, 2018.)

2.2.4 Älykäs sopimus

Älykkäät sopimukset ovat osa Blockchainin keskiötä. Vuonna 1996 tunnettu tietokoneinsinööri Nick Szabo julkaisi paperin nimeltä ”Smart Contracts: Building Blocks for Digital Markets”. Paperissan hän kuvailee älykästä sopimusta ja hänet usein mielletäänkin kyseisen konseptin pioneeriksi. Hän määrittelee älykkään sopimuksen ”kokoelmaksi lupauksia määriteltynä digitaalisessa muodossa sisältäen protokollan, jolla osapuolet suorittavat nämä lupaukset”. (Szabo, 1996) Alun perin idea ei päässyt jaloilleen yleisen mielenkiinnon puutteen vuoksi. Tämän lisäksi älykkään sopimuksen konseptista puuttui sitä toteuttava alusta. Tämä alusta löytyi vuonna 2009 Nakamoton Bitcoinin ja sitä toteuttavan Blockchain-teknologian myötä. (Mougyar, Buterin, 2016.)

Bitcoin oli kuitenkin luotu vertaisverkossa toimivaksi digitaaliseksi valuutaksi. Nakamoton Blockchain oli ensimmäinen varteenotettava hajautettu ratkaisu. Nykyään huomio on alkanut siirtyä Bitcoinin teknologian toiseen osapuoleen, eli muihin kuin Blockchain-pohjaisten kryptovaluuttojen käyttötapauksiin. (Buterin, 2014.)

Älykkäät sopimukset saivat todellista jalansijaa vasta loppuvuodesta 2013 kun Vitalik Buterin julkaisi paperinsa Ethereum-nimisestä Blockchainiin pohjautuvasta alustasta. Buterin

(2014) totesi paperissaan, että Bitcoin oli huonosti soveltuva protokolla älykkäille sopimuksille ja täten Buterinin alaisuudessa Ethereum sai alkunsa.

Älykäs sopimus on siis digitalisoitu algoritmi (yksi tapa määritellä) joka suorittaa sopimuksen ehdot. Tämä määritelmä ei kuitenkaan erota älykkäitä sopimuksia ja jo ennestään tunnettuja sopimuksenmukaisia käsitteitä toteuttaen automaattista suoritusta, esimerkiksi myyntiautomaatteja. Myyntiautomaatti voidaan määritellä itsenäisiksi koneiksi, jotka jakelevat kauppatavaraa sekä tarjoavat palveluja kolikoita syötettäessä tai luottokorttia käyttäen. Myyntiautomaatteihin on ohjelmoitu tiettyjä sääntöjä ja ne toimivat näiden sääntöjen puitteissa. (Bambara, Allen, 2017.)

Mikäli myyntiautomaattien ja älykkäiden sopimusten välillä ei ole olennaista eroavaisuutta, on älykkään sopimuksen konsepti yhtä vanha kuin itse Roomalainen laki. Kreikkalainen insinööri ja matemaatikko Heron Aleksandrialainen dokumentoi ensimmäisen myyntiautomaatin teoksessaan *Pneumatika.* Hänen laitteensa hyväksyi drakhman kolikon ja tarjosi pyhää vettä. Mennään ajassa eteenpäin 1980-luvulle, jolloin ensimmäiset finanssialan älykkäät sopimukset ohjelmoitiin Merryll Lynchin kaltaisille rahoitusalan yrityksille. Vuodesta 2014 alkaen yli 75 prosenttia pörssien kaupankäynnin kohteena olleista arvopapereista on peräisin automatisoidusta kaupankäyntijärjestelmästä. Älykkäät sopimukset eivät täten ole sinänsä uusi konsepti. (Bambara, Allen, 2017.)

William Mougyar määrittelee teoksessaan (2016) muutamia älykkään sopimuksen faktoja seuraavasti:

1. *Älykäs sopimus ei ole sama kuin sopimuksellinen sopimus*. Mikäli vetoamme Nick Szabon alkuperäiseen konseptiin, älykkäät sopimukset pyrkivät tekemään sopimuksen rikkomisen kalliiksi ohjaamalla todellisen elämän arvokasta omaisuutta ”digitalisoinnin” keinoin. Älykäs sopimus kykenee valvomaan tietyn vaatimuksen toiminnallista toteutumista ja voi täten todistaa ovatko sopimuksen ehdot täyttyneet vai ei. Nämä voivat olla suhteellisen jyrkkiä toimeenpanoja, esimerkiksi jos auton maksu ei ole ajallaan, voidaan auto lukita digitaalisesti, kunnes maksu on suoritettu.

2. *Älykkäät sopimukset eivät ole sama kuin laki.* Älykkäät sopimukset ovat tietokoneohjelmia ja täten ovat vain eräs toteutustekniikka. Kuitenkin niiden toimintojen seuraukset voivat olla osa oikeudellista sopimusta. Esimerkiksi älykäs sopimus voisi siirtää osakkeiden omistusta yhdeltä osapuolelta toiselle. Älykkään sopimuk-

sen lopputulosta voitaisiin käyttää jäljitysketjuna varmistamaan sitä, että ovatko sopimuksen ehdot täyttyneet.

3. *Älykkäät sopimukset eivät sisällä tekoälyä*. Älykkäät sopimukset ovat ohjelmistokoodia, jotka toteuttavat Blockchainissa toimivaa liiketoimintalogiikkaa. Ne käynnistetään jonkun ulkoisen datan avulla, joita käyttäen ne voivat modifioida muuta dataa.

4. *Älykkäät sopimukset eivät ole välttämättä sama asia kuin Blockchain-sovellukset*. Älykkäät sopimukset ovat yleensä osana hajautettua Blockchain-sovellusta. Yhtä tiettyä sovellusta kohti voi olla useampi sopimus. Esimerkiksi jos tietyt älykkään sopimuksen ehdot täyttyvät, ohjelma voi päivittää tietokantansa.

5. *Älykkäitä sopimuksia on suhteellisen helppo ohjelmoida*. Yksinkertaisen sopimuksen kirjoittaminen on helppoa varsinkin silloin, kun käytössä on erityistä älykkäisiin sopimuksiin suunniteltu kieli (esimerkiksi Ethereumin Solidity). Tämä mahdollistaa monimutkaisten ohjelmointiprosessien kirjoittamisen muutaman rivin muodossa.

6. *Älykkäät sopimukset eivät ole vain sovelluskehittäjille tarkoitettuja*. Seuraavan sukupolven älykkäät sopimukset ovat käyttäjäystävällisempiä, sisältäen esimerkiksi verkkoselaimen. Tämä mahdollistaa kenen tahansa yritysasiakkaan käsitellä älykkäitä sopimuksia käyttäen graafista käyttöliittymää tai vaikkapa mahdollisesti tekstipohjaista kielisyötettä.

7. *Älykkäät sopimukset ovat turvallisia*. Jopa Ethereum-pohjaisessa toteutuksessa älykkäät sopimukset pyörivät lähes Turing-täydellisinä ohjelmina. Nämä merkitsevät peruuttamattomuutta niiden suorituksessa, ja niissä ei ole loputtoman silmukan (infinite loop) riskiä.

8. *Älykkäillä sopimuksilla on monenlaisia toteuttamismahdollisuuksia ja sovelluksia.* HTML:n tavoin ohjelmat ovat rajoitettu niiden kehittäjän toimesta. Älykkäät sopimukset ovat ideaalisia reaalimaailman omaisuuden, Internet of Things:n (teollinen internet) ja taloudellisten palveluiden välineenä. Ne eivät rajoitu pelkkään rahansiirtoon. Niitä voidaan sisällyttää lähes kaikkeen mikä muuttaa tilaansa ajan myötä ja johon voi olla arvoa kiinnitettynä.
(Mougyar, Buterin, 2016.)

Suurin osa nykyajan oikeudellisista sopimuksista luodaan lakimiesten ja muiden lainoppineiden toimesta käyttäen tekstinkäsittelypohjaisia malleja. Ne sisältävät standardisoitua kieltä, jolla määritellään ehdot toteutettuna esimerkiksi Word-dokumentin muodossa. Kolmas osapuoli toimii luottotehtävissä dokumenttien tulkitsijana ja toimeenpanijana. Tämä prosessi voidaan nähdä aikaa vievänä ja tarpeettomana. Mikäli tämän lisäksi ilmenee ongelmia, turvautuvat osapuolet usein sovittelijoihin ja tuomioistuimiin tilanteen ratkaisemiksesi. (Bambara, Allen, 2017.)

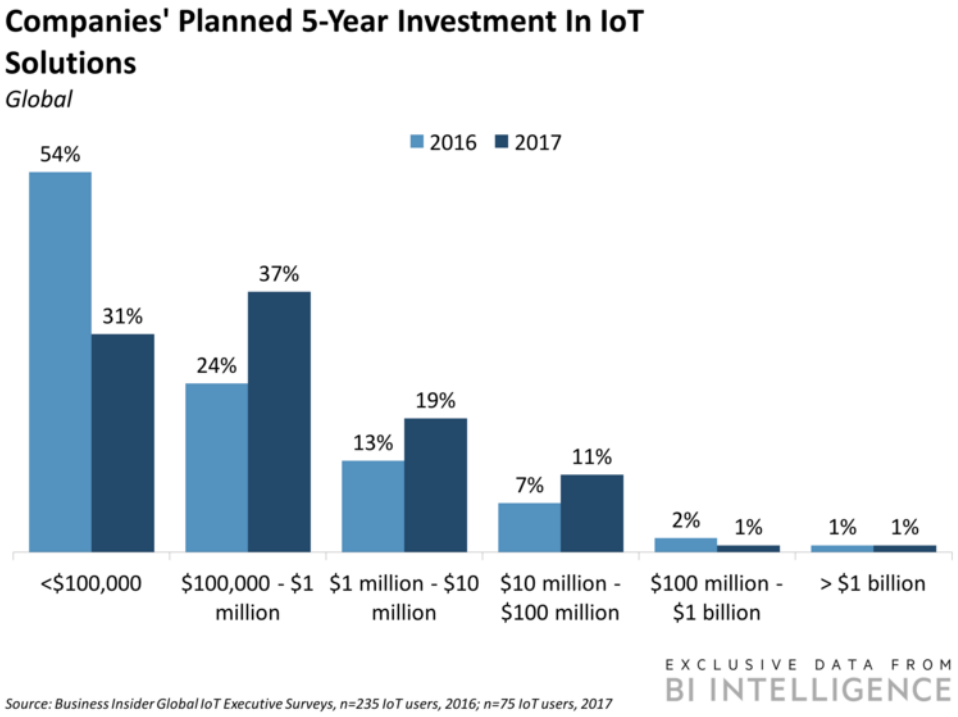
Älykäs sopimus toimii tähän ratkaisuna ja tietokoneohjelma kykenee toteuttamaan sopimuksen. Se sisältää ohjelmointikoodia, joka on kykeneväinen suorittamaan sopimuksen ehdot. Sopimuskoodi määrittelee ehdot käyttäen if/then/else –logiikkaa samalla tapaa kuin oikeudellisessa sopimuksessa. (Bambara, Allen, 2017.) Nämä ehdot voidaan validoida ja varmistaa suorittaen etämetodikutsuja (RPC calls) toisille älykkäille sopimuksille. Tällä tavoin älykkäiden sopimusten ohjelmakoodi voidaan automaattisesti suorittaa Blockchainissa. Älykkäitä sopimuksia voidaan pitää edelläkävijänä uudelle aikakaudelle, jossa asianajajat ja lainoppineet joutuvat mahdollisesti olemaan oppineita niin laissa kuin myös tietyssä määrin tietokoneohjelmoinnissa. (Bambara, Allen, 2017.)

2.2.5 Internet of Things

Aiemmin kappaleessa 2 on mainittu Gartnerin laatima nousevien teknologioiden lista kehityskäyränä. Yksi näistä teknologioista on Internet of Things (IoT) eli teollinen internet sekä siihen liittyvät sovellukset.

Internet of Things (IoT) on internetin fyysisten objektien verkosto, joka sisältää sulautettua tekniikkaa mahdollistaen laitteiden välisen kommunikaation. Tämä mahdollistaa vuorovaikutuksen muiden laitteiden kanssa sisäisesti tai ulkoisen (fyysisen) ympäristön kanssa. (Gartner, 2018) Kyseisen teknologian nopean kehityksen ansiosta IoT on avannut valtavia mahdollisuuksia uusille sovelluksille, joilla on potentiaalia muuttaa elämiemme laatua. Lähivuosina IoT on kerännyt paljon huomiota tiedemiehiltä ja ammattilaisilta ympäri maailmaa. (Xia, F., Yang, L. T., Wang, L., & Vinel, A., 2018.)

Gartner (2017) ennustaa, että 8.4 miljardia IoT-verkon laitetta on käytössä vuonna 2017, joka on 31 prosentin nousu vuodesta 2016. Vuoteen 2020 mennessä määrä on arvioidusti 20 miljardia yksikköä.



Kuva 13. Yritysten sijoitus IoT-pohjaisiin ratkaisuihin viiden vuoden aikavälillä (Gartner, 2018)

Kyseisestä kuvasta selviää suurten yritysten kiinnostus ja rahoitus IoT-pohjaisiin ratkaisuihin vuosina 2016 ja 2017, alkaen alle 100,000 dollarin sijoituksista yli miljardin dollarin sijoituksiin. (Kuva 13.)

Teollinen Internet on konseptina mielenkiintoinen, mutta Banafatin (2017) mukaan eräs IoT:n suurimmista haasteista on tietoturvallisen ekosysteemin luominen IoT:n infrastruktuurin jokaiselle osa-alueelle. Jo olemassa olevat varotoimet ja tietoturvamenetelmät ovat tärkeitä riskien pienentämisen kannalta, mutta eivät kuitenkaan riittäviä. Eräitä IoT:n tietoruvallisuuteen liittyviä haasteita ovat muun muassa huono suunnittelu ja käyttöönotto, usein turhan monimutkaiset protokollat luoden ristiriitaisia konfiguraatioita, riittävän tiedon puute sekä uusien IoT-pohjaisten ratkaisujen jatkuva eksponentiaalinen lisääntyminen – usein johtaen entistä epävarmoihin ratkaisuihin tietoturvan kannalta. (Banafat, 2017.)

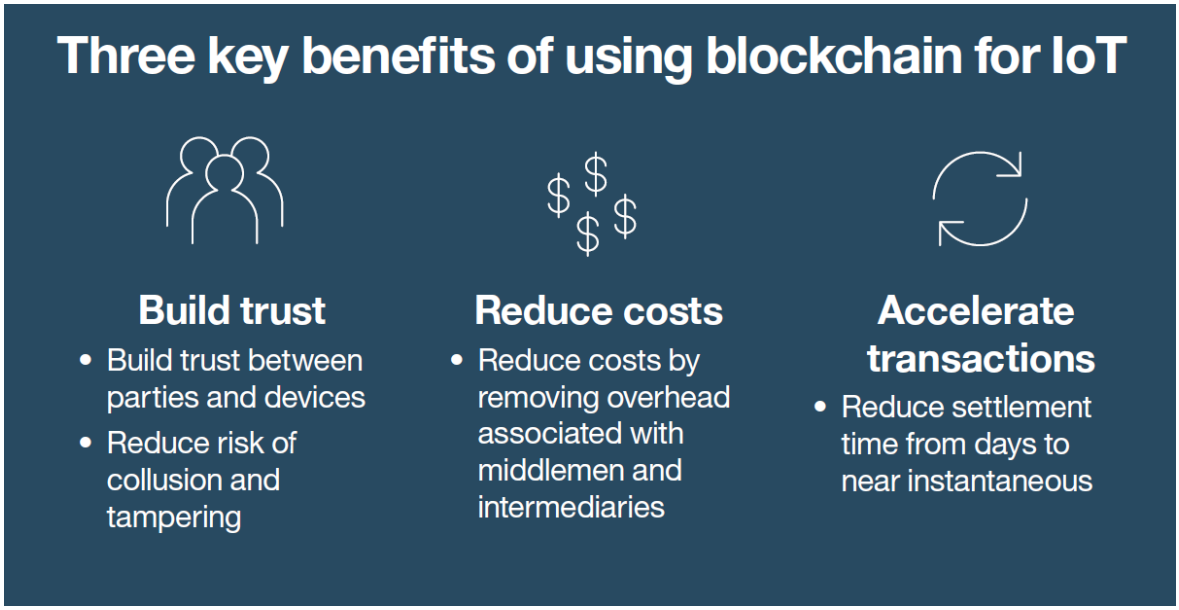
Tämänhetkiset IoT-ekosysteemit turvautuvat keskitetyn välittäjään, eli client-server-malliin. Kaikki laitteet tunnistetaan, autentikoidaan ja yhdistetään suurta prosessointi- ja talletusmuistia sisältävien pilvipalvelinten kautta. Laitteiden välinen yhteys vaatii aina internetyhteyden, vaikka laitteiden välinen etäisyys olisi vain alle muutaman metrin. Tämä malli onkin yhdistänyt yleisiä tietokoneita jo vuosikymmenten ajan ja jatkaa pienimuotoisten IoT-verkkojen tukemista tänäkin päivänä. Silti sen kapasiteetti ei riitä tulevaisuuden kasvavien ja laajojen IoT-ekosysteemien tarpeille. (Banafa, 2017.)

Kuva 14. Blockchainin ja Teollisen Internetin yhdistämisen tuomat haasteet (Banafa, 2017)

Blockchainin ja teollisen internetin integraatio ei ole kaikista hyödyistään huolimatta vailla haasteita. Muutamia haasteita, joita Blockchain-IoT -integraatio tulee varmuudella kohtaamaan ovat muun muassa skaalautuvuus, prosessointiteho, muisti, lainopilliset ongelmat sekä tietotaidon puute. (Kuva 14)

Ratkaisujen ja optimaalisten alustojen luomiseksi vaaditaan ennennäkemätöntä yhteistyötä ja koordinaatiota kaikilta ekosysteemin osa-alueilta. Kaikkien laitteiden tulee toimia yhdessä ja integroituna kaikkiin muihin laitteisiin. Lisäksi kaikkien laitteiden tulee kyetä kommunikoimaan saumattomasti kaikkien yhdistettyjen laitteiden ja infrastruktuurien kanssa. Tämä prosessi voi olla kallis, aikaa vaativa ja hankala, muttei kuitenkaan mahdoton. (Banafa, 2017)

Banafan (2017) mukaan Blockchainin ja sen tuomat edut perinteiseen järjestelmään verrattuna ovat avainasemassa tietoturvan ja luotettavuuden ongelmiin Teollisen Internetin maailmassa. Sitä voitaisiin hyödyntää miljardien yhdistettyjen laitteiden seuraamiseen, sallien transaktioiden ja laitteiden välisen koordinaation prosessoinnin. Tämä mahdollistaa huomattavia säästöjä Teollisen Internetin tuottajille. Hajautettu malli karsisi yksittäiset vikatilanteet, luoden vastustuskykyisiä ekosysteemejä laitteiden alustoiksi. Blockchainien käyttämät algoritmit suojaisivat kuluttajien yksityisyyttä ja tietoja paremmin. (Banafa, 2017.)



Kuva 15. Kolme avainhyötyä Blockchainin käytöstä teollisessa internetissä (IBM, 2016)

Yllä oleva kuva selittää kolme tärkeintä hyötyä jota Blockchain tuo Teollisen Internetin maailmaan. Ensimmäisenä mainitaan luottamuksen luominen. Käytännössä tällä tarkoitetaan luottamuksen luomista osapuolien ja laitteiden välillä. Lisäksi vähennetään väärinkäytön riskiä. Toisena hyötynä mainitaan taloudellinen hyöty. Blockchain integroituna teolliseen internettiin tuo huomattavia leikkauksia kolmansiin osapuoliin ja välikäsiin liittyviin yleiskuluihin. Viimeisenä hyötynä mainitaan liiketapahtumien nopeuttaminen käyttämällä Blockchain-integroitua ioT-alustaa. Tällä saadaan vähennettyä suoritusaikoja päivistä lähes välittömiin nopeuksiin. (IBM, 2016.)

Eräs Blockchainin ja Teollisen Internetin integraation tuomien hyötyjen puolestapuhujista on teknologiajätti IBM. Sen yksityinen Blockchain on hajautetuista solmuista koostuva infrastruktuuri, joka jäljittelee laitedataa ja validoi liiketapahtumat käyttäen älykkäitä sopimuksia. Käyttöoikeutettu Blockchain mahdollistaa käyttäjien hallinnoinnin ja rajauksen, sallien liiketoimintaverkoston osanottajien näkevän vain sen osan Blockchainin sisältöä, joihin heillä on käyttöoikeus. Tämä infrastruktuuri auttaa vakiinnuttamaan luotettavuutta, vastuuta ja läpinäkyvyyttä, samalla tehostaen nykyisiä prosesseja ja sallien uusia liiketoimintamalleja. (IBM, 2016)

IDC:n laatiman tutkimuksen mukaan 20 prosenttia käyttöönotetuista Teollisen Internetin ratkaisuista tulee sisältämään Blockchainin integraation vuoteen 2019 mennessä. (I-Scoop, 2018)

3 Tutkimustapaukset ja analyysi - Energiateollisuus

Kappaleessa käydään ensiksi läpi sekä kuvaillaan tutkimuksen kohteeksi valittuja käyttötapauksia. Tutkimustapaukset liittyvät energiateollisuuteen tutkien sitä, että voidaanko Blockchainia mahdollisesti hyödyntää kyseisellä alalla. Tutkimustapaukset rajautuvat energiayritys Fortumiin, joka on tutkimuksen kohteena. Tämän jälkeen käydään läpi ja analysoidaan kerättyä tutkimusdataa.

Eurelectricin (2018) tuottaman tutkimuksen mukaan Blockchainin suurin potentiaali on sektoreissa, joissa osapuolten välinen fyysinen transaktio ei ole tarpeellinen. Näihin kuuluvat muun muassa finanssisektori. Tämän kaltaisissa sektoreissa Blockchainin avulla voidaan tuottaa luotettavaa dokumentaatiota ilman tarvetta fyysisen transaktion varmistamiselle. Kuitenkin tiettyihin sektoreihin sisältyy fyysinen transaktio. Näissä energiateollisuus on muita paremmin soveltuva käyttökohde Blockchain-integraatiolle. Sähkön osto- ja myynti selvitetään kokonaisuutena keskitetyissä kaupankäyntijärjestelmissä, kuten finanssisektorin tapauksessa pörsseissä ja muissa rahoitusmarkkinaympäristöissä.

ETLAN (2016) teettämän tutkimuksen mukaan Blockchainin olennainen valtti on sen kyky ylläpitää konsensusta tietokantojen sisällöstä, jotka on jaettu toistensa tuntemattomien tasa-arvoisten solmujen välillä. Blockchain-pohjaiset ratkaisut sopivat erityisen hyvin tietokantoihin, joissa kaikki voivat käyttää kaikkia tietoja, mutta kukaan osapuoli ei voi täysin hallita sitä, kuinka ja kuka tietokantaa voi muokata. (Mattila ym. 2016)

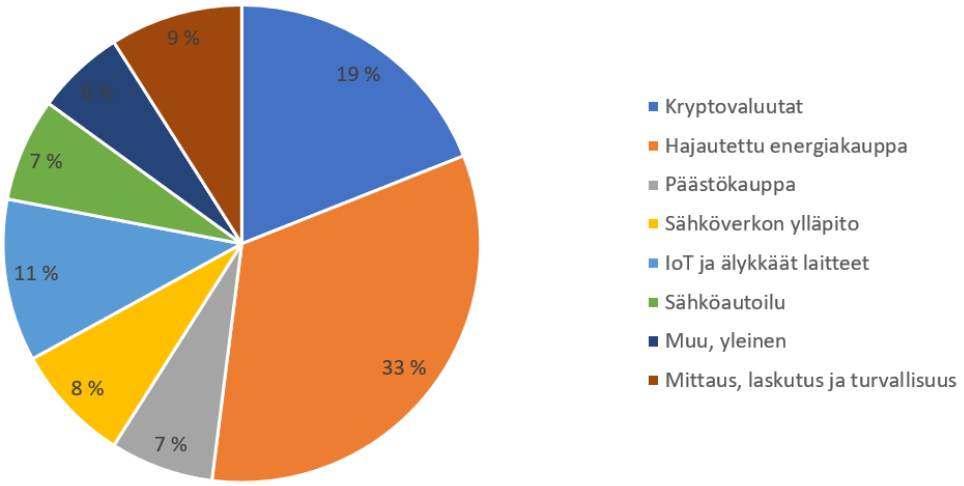
Blockchainin eräänä tärkeänä käyttökohteena voidaan nähdä energiateollisuus. PwC:n (2016) teettämän tutkimuksen mukaan useampi yritys kehittelee tällä hetkellä Blockchain-pohjaisia sovelluksia energiateollisuuden alalle. Kaikki sovellukset on lähtökohtaisesti suunniteltu tuottajien ja kuluttajien yhdistämiseen, luoden tai tarjoten suoran yhteyden molempien osapuolen välille. (Hasse ym. 2016)

Joitain Blockchainin finanssialan peruskäsitteitä voidaan soveltaa myös energiateollisuudessa. Muutamana esimerkkinä voidaan mainita hajautettu data lisäten turvallisuutta sekä älykkäiden sopimusten integraatio. (Hasse ym. 2016) Yleisesti ottaen energiateollisuuden käyttötapaukset voidaan jakaa kolmeen sovelluskategoriaan. Nämä sovellukset keskittyvät muun muassa seuraaviin asioihin:

- Liiketapahtumiin sekä älykkäisiin sopimuksiin – Hajautettu energian myynti ja osto (pääasiassa sähkö), sähköinen liikkuvuus (Electric mobility), älykkäät laitteet, kryptovaluuttojen integraatio

- Omistajuuden dokumentointiin – Rekisterin ylläpito, alkuperän takaus, uusiutuvan energian sekä päästöoikeuksien sertifikaatit
- Hajautettujen liiketapahtumien dokumentointiin – Energiakulutuksen, lämpökulutuksen, sekä sähköisen liikkuvuuden (sähköautot) mittaaminen ja laskutus (Hasse ym. 2016)

Tuoreessa tutkimuksessa Ruotsin Fortumin tutkimus- ja tuotekehityspäällikkö Catarina Naucler (2017) kertoo Blockchainin potentiaalista energiantuotannon alalla. Fortumin Blockchainin käyttötapausten tulevaisuuden visioihin/tutkimustyön kohteisiin sisältyvät muun muassa ylijäämäenergian jakelu vertaisverkossa, IoT-pohjainen älykäs koti -konsepti, sekä sähköautoilu (EV). (Naucler, 2017.)



Kuva 16. Blockchainin käyttötapaukset energiateollisuudessa aktiivisuuden mukaan (Andoni ym. 2019)

Yllä oleva kaavio ilmaisee sitä mihin erilaisiin käyttötapauksiin Blockchainia on hyödynnetty tähän mennessä. Käyttötapaukset on luokiteltu aktiivisuuden mukaan. Tutkimus perustuu 140 eri Blockchainiin perustuviin hankkeisiin. Näihin 140:een sisältyvät erilaiset suuremmat- ja startup-yritykset, sekä tutkimuslaitokset. (Andoni ym. 2019)

Tutkimuksesta selviää, että 33 prosenttia (kolmannes) kaikista energiateollisuuden käyttötapauksista liittyy hajautettuun energiakauppaan. Tähän kuuluvat muun muassa tukku-, vähittäiskauppa- sekä vertaisverkossa (P2P) toimiva energianjakelu. (Kuva 16) Tämä osoittaa selkeää kiinnostusta eri sidosryhmiltä vertaisverkossa toimivaa energianjakelua kohtaan.

Fortum on teettänyt Blockchainista useamman diplomityön, sekä kirjoittanut aiheesta tutkimuksen nimeltä Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry. Tutkimus on tuotettu vuonna 2016 yhdessä ETLAN kanssa.

Tämän lisäksi Fortum on ollut mukana mm. Tekesin BOND (Blockchains Boosting Finnish Industry) -projektissa vuosina 2016-2018. Tämän lisäksi Fortum on ollut mukana muun muassa Innogyn ja Enelin kanssa Blockcharge-pilotissa (Oslo2Rome) ja Eurelectricin kautta. (Stahl 24.9.2018.) Hankkeen kokonaisvaltaisena tavoitteena oli muodostaa ymmärrystä Blockchain-pohjaisille työkaluille, teknologioille, sekä liiketoimintamahdollisuuksille eri osa-alueilla, kuitenkin keskittyen Suomalaiseen liiketoimintaan. (ETLA 2016.)

3.1.1 Käyttötapaus: Sähköautojen latausinfrastruktuuri ja Blockchain

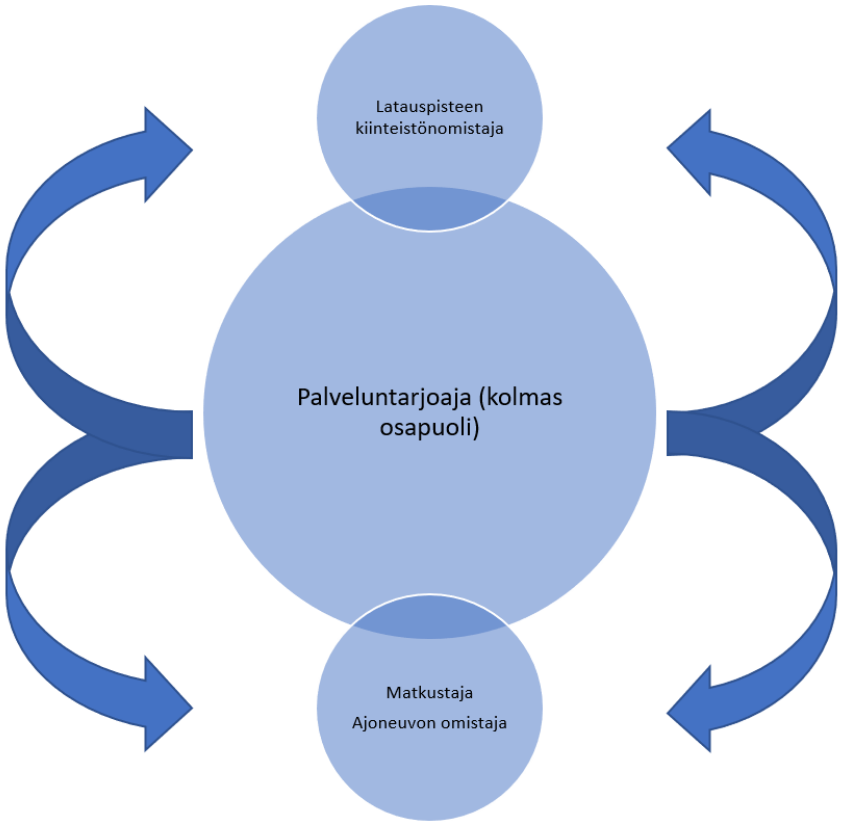
Eräs potentiaalinen käyttötapaus liittyy sähköautoiluun ja sitä ympäröivään latausinfrastruktuuriin. Sähköautojen (EV) suosion ja merkittävyyden kasvaessa järjestelmäoperaattorit kohtaavat uusia haasteita. Muun muassa uuteen sähköautoiluun liittyvä liikkuva kuorma ja ylijäämävarastoidun energian käyttäminen joustavuuden parantamiseksi ovat keskeisiä haasteita sähköautoilulle. Blockchain voisi parantaa EV-latauksen koordinointia helpottamalla energiamaksuja latausasemilla sekä antamalla kuljettajille mahdollisuuden tehdä latauspäätöksiä karttojen ja reaaliaikaisten hintatietojen perusteella. (Eurelectric 2018)

Blockchainia voidaan käyttää kehittämään sähköautojen ekosysteemiä ja niitten lataamiseen liittyvää infrastruktuuria. Waterloon Yliopiston (2019) teettämän tutkimuksen mukaan sähköautojen lataamisen mahdollistavien palveluntarjoajien, latauspisteen kiinteistön omistajien, sekä sähköautojen (EV) omistajien välillä vallitsee epäluottamuksen ilmapiiri. Ongelmaksi ilmenee täten kolmas osapuoli.

Blockchainin avulla voitaisiin poistaa tämä ongelma tehden alustasta julkisen. Kaikilla osapuolilla on avoin pääsy tarkastelemaan dataa ja havaitsemaan mahdolliset virhetilanteet. Kiistatilanteissa osapuolet voivat havaita selkeästi, mikäli esimerkiksi sähköautojen omistajia on veloitettu liikaa, tai kiinteistön omistajia veloitettu liian vähän. Waterloon Yliopiston tutkimuksen mukaan tämä skenaario voisi olla luotettava vaihtoehto keskitetylle järjestelmälle, mahdollistaen muun muassa energian jakelun vertaisverkossa. (University of Waterloo, 2019.)

Perinteiset energiateknologiat ovat luonteeltaan keskitettyjä ja niiden välillä vallitsee yleisesti ottaen luottamus. Nykypäivänä kuitenkin energiateknologioista on tullut enemmän ja

enemmän hajautettuja. Syynä tähän on kehitys muun muassa hajautetuissa uusiutuvien energialähteiden tuotossa, säilöntäteknologioissa, sekä sähköautoilussa. Näissä uusissa järjestelmissä energiapalveluja tuotetaan usein kokonaisuuksilla, joilla ei ole vakiintunutta luottamussuhdetta asiakkaiden ja muiden osapuolten välillä. (Gorenflo ym. 2019) Tutkimuksessa selviää, että sähköautoilu (EV) sekä sitä ympäröivä infrastruktuuri ovat luontaisia käyttötapauksia Blockchainille ja älykkäille sopimuksille. Liikenteen hajautettu luonne sisältää useita sidosryhmiä (kuski, matkustaja, auto, latausasemat jne.). Tämä tekee Blockchainista luonnollisen käyttötapauksen sähköautoilussa. Tässä tapauksessa hajautetusta mallista on hyötyä muun muassa siinä, että tarve keskistetysti valvotulle sähköauton latausinfrastruktuurille poistuu. Lisäksi vikasietokyky (Fault Tolerance, kappale 2.1.4), sekä selkeät hinnoittelut sidosryhmien välillä vähentävät kiistatilanteita muun muassa hinnoittelussa.



Kuva 17. Sähköautoilun infrastruktuurin keskitetty, kolmannen osapuolen hallinnoima malli.

Yllä olevassa kuvassa esitellään perinteinen, kolmanteen osapuoleen nojautuva markkinarakenne. Sidosryhmien välillä tulisi optimaalisesti olla täydellinen yhteisymmärrys muun muassa hinnoittelun suhteen. Käytännössä kuitenkaan tämä harvoin toteutuu ja täten kiistatilanteita voi syntyä sidosryhmien välille. (Kuva 17).

Tutkimuksen perusteella selviää kuitenkin, että Blockchainin hyödyntäminen sähköautoilun infrastruktuurissa ei tule ilman haasteita tai rajoitteita. Eräs olennainen haaste liittyy henkilötietojen salaamiseen ja tietoturvaan yleisesti.

Jotta Blockchainin ja energiateollisuuden integraatio olisi onnistunutta, vaaditaan muutamia askelia. Ensimmäisenä tulee selvittää osalliset sidosryhmät ja heidän luottamuksensa taso toisiansa kohtaan. Luottamuksen taso voi olla puutteellista sidosryhmien välisissä suhteissa, kun pyritään löytämään sovelluksen optimaalista käyttötapaa. (University of Waterloo, 2019.)

Tämän lisäksi Blockchain-järjestelmän tulisi hyödyntää älykkäitä sopimuksia. Termillä viitattiin ohjelmoituihin algoritmeihin, joilla voidaan tehokkaasti validoida sopimuksen ehtojen täyttymistä digitaalisesti. Älykkäiden sopimusten avulla voidaan ratkaista yllämainittuja luottamukseen liittyviä haasteita. Kappaleessa 2.2.4 puhutaan älykkäistä sopimuksista. Kaikki kanssakäymiset sidosryhmien välillä voidaan käsitellä Blockchainin lohkoketjussa. Sen sijaan että datan analysoinnissa turvaudutaan erillisiin mittareihin, kulkisi data Blockchainin lohkon kautta. Älykäs sopimus mahdollistaa automaattisen auditoinnin prosesseille ja liiketapahtumille. (University of Waterloo, 2019.)

Eräs aktiivinen projekti tällä osa-alueella on MotionWerkin Share&Charge -projekti. Vuonna 2016 Innogy (Saksalaisen energiayhtiö RWE:n tytäryhtiö) päätyi yhteistyöhön Saksalaisen Blockchain-startup Slock.it:n kanssa. Heidän yhteisenä tavoitteenaan oli luoda vertaisverkkoon pohjautuva P2P-palvelu, jonka avulla sähköautojen ja latauspisteiden omistajat voivat vuokrata latausinfrastruktuurinsa toisilleen itsenäisesti ilman kolmannen osapuolen välittäjän tarvetta. Toukokuuhun 2017 mennessä Innogyn innovaatiohautomo oli tuottanut uuden startup-yrityksen, MotionWerkin. Sen ensimmäinen luomus, Share&Charge, mahdollisti EV-omistajille oman ajoneuvonsa lataamisen suorittamalla digitaaliasia maksuja mobiilisovelluksen avulla. Latauspisteiden omistajat käyttivät sovellusta asettaakseen heidän infrastruktuurinsa saataville, tullimaksujen rakenteiden asettamiseen, sekä maksujen keräämiseen. (Eurelectric 2018)

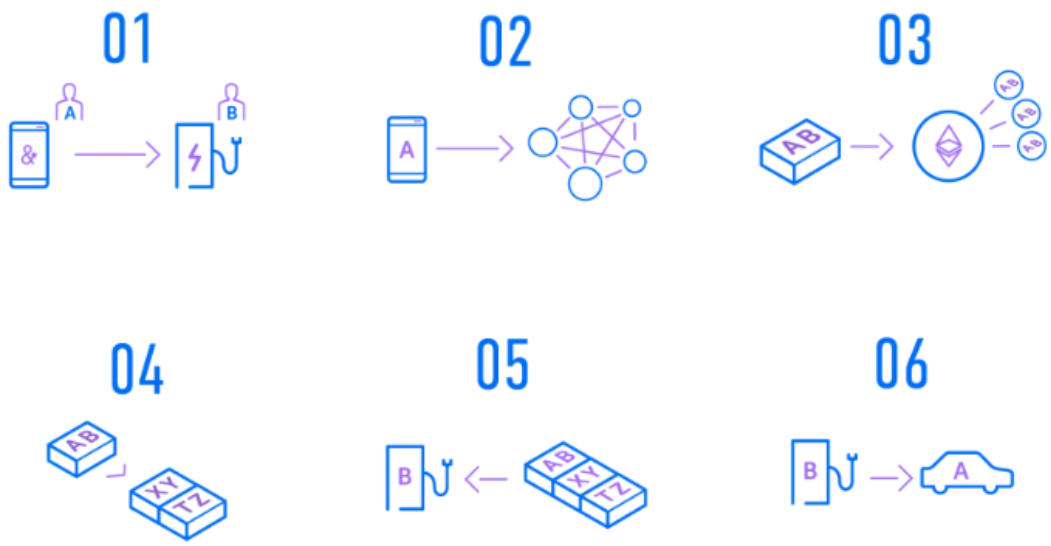
Huhtikuuhun 2018 mennessä palvelu oli saatavilla noin 1 000 EV-omistajalla, joiden käytössä oli 1 250 yksityistä ja julkista latauspistettä Saksassa. Järjestelmä käytti digitaalista lompakkoa (”E-Wallet”) ja älykkäitä sopimuksia julkisessa Ethereumin lohkoketjussa P2P-liiketapahtumatasona, mukaan lukien euron tukemaa ”Mobility Tokenia”. (Eurelectric 2018)

Share&Charge oli maailman ensimmäinen sähköisen liikkuvuuden (”E-Mobility”) transaktioalusta, joka käytti hyödykseen Blockchainia. Perustuen loppukäyttäjäkokemuksiin sekä MotionWerkin toteuttamiin eri kokeiluihin (esimerkiksi Oslo2Rome -projekti, jossa Suomalainen Fortum ollut mukana toteuttamassa), Share&Charge on tällä hetkellä muuttumassa sähköautojen latausinfrastruktuurin avoimen lähdekoodin hajautetuksi digitaaliseksi protokollaksi. Sen tarkoituksena on tarjota latauspisteen ylläpitäjille ja sähköisen liikkuvuuden (E-Mobility) palveluntarjoajille mahdollisuus hajauttaa voimavaransa muiden etujen ohella. Näitä etuja ovat EV-infrastruktuurin valvonnan, maksutoimintojen, sekä suoritusten yksinkertaistaminen. (Eurelectric 2018)

Suomalainen energiayhtiö Fortum on ollut osallisena muassa Innogyn ja Enelin kanssa toteutetuissa Blockchain-pilotoinneissa (muun muassa Share&Charge sekä Oslo2Rome). Sähköautojen osalta Blockchain on yksi ratkaisu ns. Roaming-maksujen poistamiseksi ja mahdollistaa näin sähköautojen latauksen eri maissa ilman lisäkustannuksia tai kolmansia osapuolia. (Stahl 24.9.2018.)

Stalhl (2018) kertoo, että Oslo2Rome oli yhteistyöhanke seitsemän Eurooppalaisen kumppanin kanssa, tavoitteenaan ottaa käyttöön maiden rajojen välinen Blockchainiin perustuva roaming-mallinen ladattava sähköverkko käyttäen ”E-mobility wallet” -viitekehystä. Pilotti oli kaikilta osin onnistunut, ja jokainen osallistuja pääsi kohteeseensa käyttäen Euroopan laajuista Blockchainilla toimivaa latausverkkoa. Oslo2Rome -aloite todisti, että Blockchain-pohjainen ratkaisu voisi ratkaista roaming-malliin liittyviä ongelmia Euroopan sähköautojen latausverkoissa.

Oslo2Rome -projekti mahdollistaa reaaliaikaiset liiketapahtumat ja suoritukset ilman välikäsiä käyttäen Blockchainin älykkäitä sopimuksia. Menetelmä on sopimukseton, eli se mahdollistaa pääsyn ja maksamisen ilman sopimuksia tai käyttäen roaming-mallia, joka hyödyntää Blockchain-pohjaista lompakkoa (E-mobility wallet). Tämä on helppo ja kustannustehokas omaisuusintegraatio, jonka toiminta perustuu yhteensopivaan ja hajautettuun Blockchain-verkostoon. (Share&Charge 2019.)



Kuva 18. Oslo2Rome -pilotin toimintaperiaate vaihe vaiheelta (Share&Charge 2019)

Aluksi käyttäjä A (tässä tapauksessa sähköautoilija) haluaa käyttää Share&Charge -sovellusta ladatakseen autoaan käyttäjän B latausasemassa. Sovellus sitten lähettää aloituskäskyn Blockchain-verkostoon. Kolmannessa vaiheessa aloituskäsky lisätään uuteen Blockchain-lohkoon. Tämä uusi lohko jaetaan kaikkien kyseisen hajautetun Ethrereum-Blockchainin osanottajille. Nämä osanottajat validoivat lohkon. Tämän jälkeen lohko lisätään osaksi Blockchain-lohkoketjua, luoden läpinäkyvän ja muuttumattoman dokumentaation lataustapahtumalle. Latausasema käy läpi kaikki tuoreet transaktiot Blockchainissa, löytäen aloituskäskyn. Lopuksi käyttäjä A voi aloittaa latauksen. (Share&Charge 2019.)

Fortum on jo testannut sähköautojen latausta Blockchainilla Tukholman ja Oslon välillä, mikä on hyvinkin todennäköinen käyttökohde tulevaisuudessa. Uusiutuvilla on tehty kauppaa Blockchainia hyödyntäen muun muassa New Yorkissa, joten myös se on hyvinkin todennäköinen tapa tehdä kauppaa paikoissa, joissa ei ole regulaation tuomia esteitä ja/tai muuta kauppapaikkaa ei ole. Myös Saksassa Blockchainia on hyödynnetty alueelliseen uusiutuvien kauppaan, koska Blockchain voi tarjota alkuperätakuun tuotetulle sähkölle. (Stahl 24.9.2018.)

3.1.2 Käyttötapaus: Energianjakelu hyödyntäen Blockchainia

Kappaleessa on mainittu aiemmin, että 33 prosenttia kaikista energiateollisuuden käyttötapauksista liittyy hajautettuun energiakauppaan. Tähän kuuluvat muun muassa tukku-, vähittäiskauppa- sekä vertaisverkossa (P2P) toimivaan energian jakeluun.

Energian jakelun ja myynnin perinteiset prosessit ovat monimutkaisia ja osittain epäkäytännölliseksi todettuja. Blockchainiin perustuva hajautettu jakelumalli voisi vähentää liiketoimintakuluja energiateollisuuden tukkumyynnissä. Sähkön vähittäisjakelun/jälleenmyynnin tapauksessa Blockchainin avulla voidaan laskea muuttujakuluja vähittäismyynnin maksuprosessoinnissa sekä kirjanpidossa. Tämän lisäksi laskutukseen liittyvää läpinäkyvyyttä voidaan nostaa. Energiasopimuksen solmimisen sekä lopettamisen prosesseja voidaan optimoida vähentämällä byrokratiaa. Tällä myös mahdollistetaan asiakkaalle laajempi valikoima energian tarjontaa. (Eurelectric 2018)

Blockchain mahdollistaa Peer-to-Peer (P2P) -mallisen jakeluverkoston, jossa energiaa voidaan myydä ja jaella vaikkapa naapureille käyttäen hyväksi älykkäitä sopimuksia. Tällä voidaan ottaa taakkaa pois perinteisestä energian siirtoverkostosta. Täten saadaan optimoitua hajautettua energiatuotantotaloutta paremmin. (Eurelectric 2018)

Perinteisessä skenaariossa sähkö- ja polttoaineen tukkukaupassa kaupat aloitetaan välittäjän kautta tai pörssissä. Ennen tätä tulee kauppiaan kuitenkin konsultoida indeksilaitosta hintatietojen keräämistä varten. Kun kauppa on lyöty lukkoon, molemmat osapuolet erikseen lisäävät tapahtuneen kaupan tiedot omiin IT-järjestelmiinsä. Näitä järjestelmiä kutsutaan yleisesti nimellä ETRM eli ”Energy Trading and Risk Management” (energiakauppa ja riskienhallinta). Kummankin osapuolen IT-osastot noutavat tapahtuman yksityiskohdat omista ETRM-järjestelmistään, varmistaen tietoja keskenään ja välittäjän kanssa kaupan vahvistamiseksi ja sovittamiseksi. Tämä vaihe saavutetaan joko automatisoiduilla vahvistusjärjestelmillä, kuten EFETnet (European Federation of Energy Traders) Euroopassa, tai perinteisillä viestintäkanavilla (sähköposti, puhelut, faksi) sekä laskentataulukoilla. (Eurelectric 2018)

Kauppa saatetaan sitten päätökseen fyysisesti siirtoverkonhaltijan eli TSO:n (transmission system operator) kautta. Kauppa selvitetään taloudellisesti myös selvityslaitoksen tai pankin kautta. Lopuksi molemmat toimijat ilmoittavat tapahtuman yksityiskohdat asianomaisille tilintarkastajille ja sääntelevilleelimille velvollisuuksien ja standardien mukaisesti. (Eurelectric 2018)

Tämä prosessi sisältää epäkäytännöllisiä ja huonosti kommunikoinnin mahdollistavia IT-järjestelmiä. Tästä voi seurata muun muassa korkeita liiketoimintakuluja (korkeat vaihto- ja välityspalkkiot, hinnoittelulaitosten palkkiot) sekä korkeita operatiivisia kuluja. Blockchain-pohjainen alusta voisi vähentää suuren volyymin kauppojen liiketoimintakustannuksia tehostamalla toimintaprosesseja ja yhdistämällä kaikkien osapuolten kaupankäyntialustat. Jotkut näkevät Blockchain-pohjaisten kauppapaikkojen poistavan välittäjien

ja selvityslaitosten tarpeen. Lisäksi Blockchainin avulla voitaisiin mahdollistaa osallistujille kaupankäynti pienemmissä volyymeissä vähentämällä transaktiokustannuksia. (Eurelectric 2018)

Fortum on ollut yhteistyössä Eurelectricin kanssa Blockchain-pohjaisten käyttötapausten tutkimuksessa. Eräs yhdessä toteutettu projekti on Pontonin pilotoima Enerchain-hanke. Enerchainin kaltaiset alustat pyrkivät alentamaan energian tukkukauppaan liittyviä kuluja. Se toimii selvitysalustana tukkukaupan liiketapahtumille, jotka eivät turvaudu keskitettyihin toimijoihin tai välittäjiin. Enerchain antaa energian tukkumyyjille mahdollisuuden lähettää nimettömästi tilauksia hajautettuun ”tilauskirjaan”, johon myös muut kauppiaat pääsevät käsiksi. Enerchain-alustassa tapahtuvien liiketapahtumien volyymi kokonaisluvuissa on vielä paljon pienempää kuin Euroopan johtavan energiavirasto EEX:n (European Energy Exchange) volyymi. Enerchain on kuitenkin laajentunut tuntuvasti. Vuonna 2017 se aloitti 15 energianjakeluyrityksen konsortiona. Huhtikuuhun 2018 mennessä se oli kasvanut jo 42 yrityksen kokoiseksi konsortioksi. (Eurelectric 2018)

Samalla lailla kuten tukkukaupassa, Blockchain voisi parantaa sähköenergian vähittäismyynnin markkinoita käyttämällä kryptovaluuttoja laskutuksen selvittämiseen ja muihin ”meter-to-cash” (M2C, älykkäiden mittarien ylläpitoalusta) -mallisiin prosesseihin. Mahdollistamalla kauppojen välittömän selvityksen Blockchainia voitaisiin käyttää vähentämään maksujen käsittelyyn ja kirjanpitoon liittyviä muuttuvia kustannuksia. Nämä toiminnot voitaisiin toteuttaa käyttämällä älykkäitä sopimuksia. Joidenkin tahojen mukaan Blockchainiin perustuva M2C-automaatio poistaisi sekä tukku- että vähittäismyynnistä kolmansien osapuolien välittäjien tarpeen kokonaan. Blockchain voisi auttaa vähittäisasiakkaita taloudellisesti mahdollistamalla suuremman avoimuuden energiamaksuissa ja laskutuksen vaiheissa, sekä mahdollisuudessa sopia ja purkaa energiasopimuksia sulavammin. Lisäksi voidaan tehostaa toimintaa lisäämällä valinnanvaraa sekä läpinäkyvyyttä energiantoimituksessa. (Eurelectric 2018)

Blockchain voisi mahdollistaa vertaisverkkojen (P2P) markkinoiden kehityksen, jossa energiantuottajat ja kuluttajat käyvät kauppaa paikallisella tasolla. Mahdollistamalla paikalliset markkinat Blockchain voisi vähentää siirtoverkkojen kuormitusta (vähentäen verkon kustannuksia), ja täten parantaa pienimuotoisten uusiutuvien energialähteiden sekä hajautettujen energiaresurssien (DER, distributed energy resources) taloudellisuutta ja avoimuutta energiantoimituksessa. Suuri osa Blockchainin painopisteestä energiateollisuudessa on keskittynyt juuri vertaisverkossa toimivien P2P-energiamarkkinoiden mahdollistamiseen. Tuoreen tutkimuksen mukaan 57 prosenttia Blockchainin rahoituksesta ener-

giateollisuudessa käytetään Blockchainin hyödyntämiseen vertaisverkossa toimivien transaktioiden nopeuttamiseen sekä parempaan verifikointiin. (Eurelectric 2018)

Yleinen lähestymistapa sähkön kauppaan Blockchainilla – vertaisverkkomarkkinoilla ja muualla – edellyttää viestintälaitteiden tai Blockchain-verkkoon kytketyn tietokoneen sovittamista älykkääseen sähkömittariin. Älykäs mittari ja Blockchain toimivat vuorovaikutuksessa ja ovat tietoisia toisistaan. Blockchainin kanssa vuorovaikutuksessa oleva älykäs mittari toimii yhteyspisteenä ja vahvistajana sähköjärjestelmän ja Blockchainin välillä. Mittari kirjaa sähköntuotannon, tuonnin ja viennin.

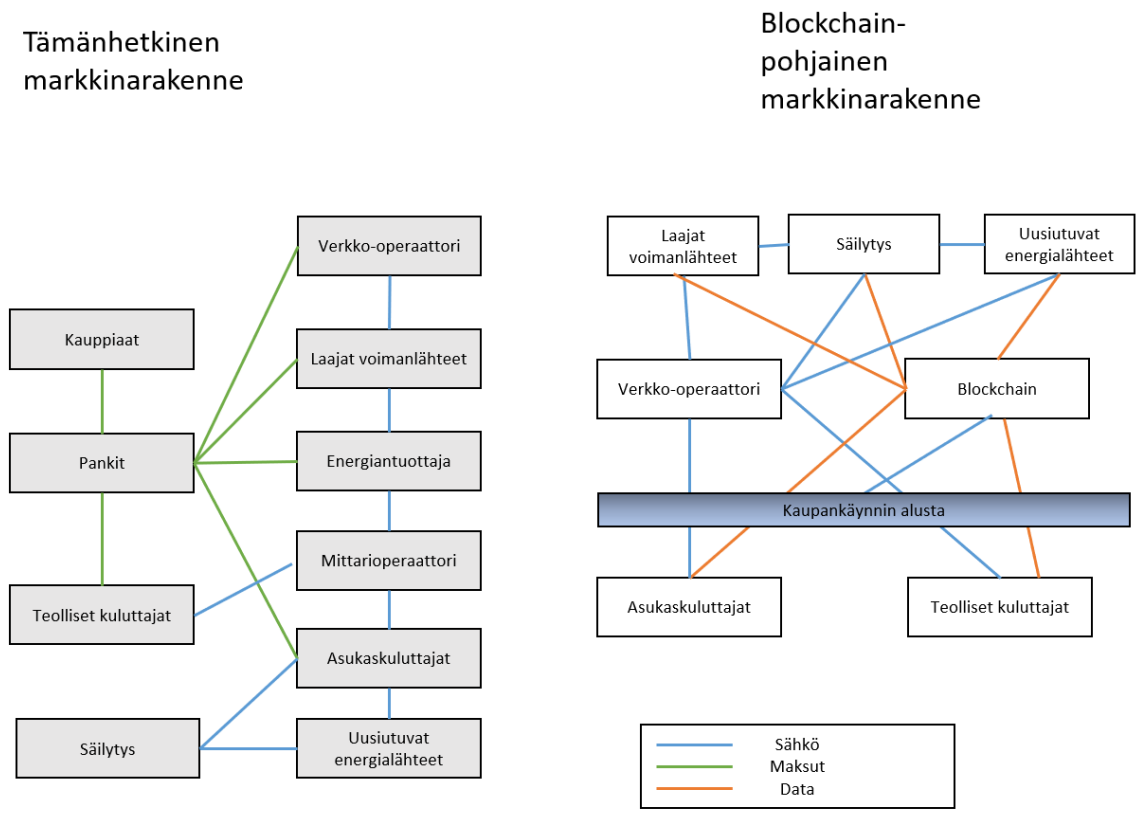
Tämä muunnetaan ”tokeneiksi” jotka edustavat varoja tai rahallista arvoa. Kauppojen tapahtuessa nämä allokoidaan markkinaosapuolille liittämällä transaktiot Blockchainiin. Näitä kolikoita säilytetään ”e-lompakossa” (E-wallet) ja niitä voidaan hankkia sekä lunastaa käyttäen Fiat-rahaa tai kryptovaluuttaa. (Eurelectric 2018)

Tulevaisuuden energiajärjestelmässä tulee olemaan aikoja, jolloin energiaa tuotetaan liikaa (aurinkoinen ja tuulinen päivä), sekä aikoja, jolloin energiaa on liian vähän (kylmä ja tuuleton päivä). Avainkysymyksenä liittyen uuteen energiamalliin on ratkaista se, että energian tuotto ja kulutus ovat tasapainossa. Jotta tähän kysymykseen voidaan saada vastaus, on kaikkien resurssien joustavuuden lisääminen välttämätöntä. Jossain osa-alueissa hajautettu energiajärjestelmä voisi olla rajoitteena paikalliselle sähköverkolle, siinä missä EV (sähköautot) ja PV (photo-voltaic, aurinkokennot) toimisivat uusina paikallisina energialähteinä. (Hasse ym. 2016)

Aurinkovoima ei mahdollista tarpeeksi suurta tuotantokapasiteettia, joten vaaditaan verkkosähköyhteys. Aurinkovoimasta saadaan korkeammat tuotot, jos energia siirretään säilömisen sijasta verkkoon.

Tämän vuoksi yksi tavoitteista on se, että yksiköt voisivat jaella sähköä keskenään itsenäisesti. Näin jakelusta saataisiin tehokasta, itsenäistä ja ulkoisista osapuolista riippumatonta. Joitakin aiempia käyttötapauksia on kaavailtu. Näissä on keskitytty jakamaan hajautettuja uusiutuvan energian resursseja naapuritalouksien välillä Blockchainin avulla. Osaa näistä on toteutettu käytännössä. (Hasse ym. 2016)

Blockchain-pohjaiset prosessit eivät enää vaatisi energiayhtiöitä tai pankkeja maksutapahtumien valvonnassa. Sen sijaan hajautettu energianjakelu- ja tarjontajärjestelmä tukisi ekosysteemiä käyttäen Blockchainiin pohjautuvia älykkäitä sopimuksia. Tämä sallisi kuluttajien hallinnoida omia energiasaantisopimuksia sekä kulutusdataa. (Hasse ym. 2016)



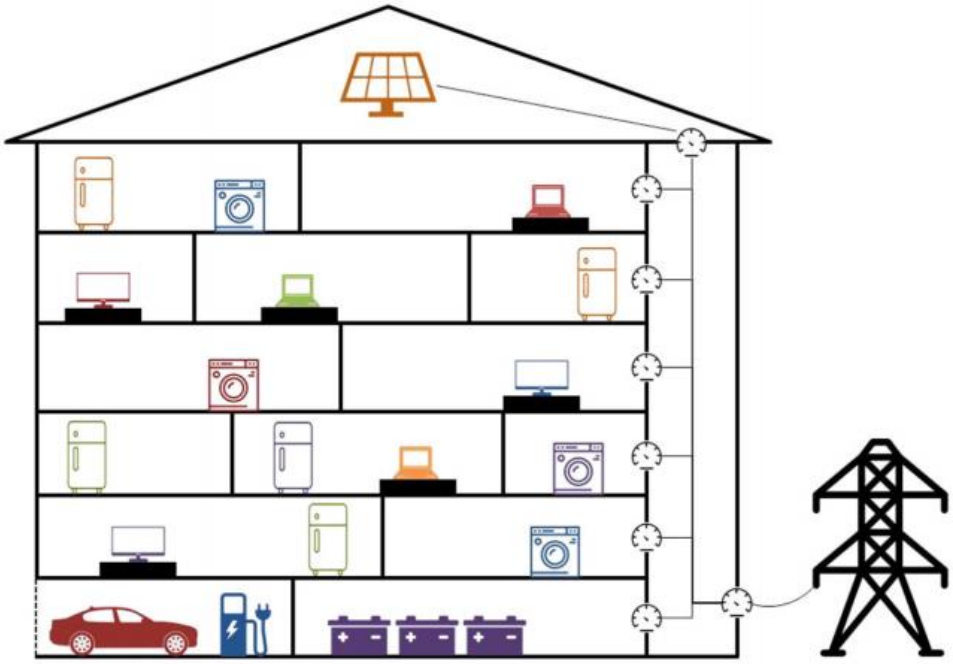
Kuva 19. Perinteinen, sekä Blockchain-pohjainen markkinarakenne (Andoni ym. 2019)

Kaaviossa esitellään PwC:n (2016) tutkimukseen pohjautuva rinnakkainen vertailu, jossa vertaillaan kahta prosessikuvausta. Vasemmalla esitellään perinteistä prosessikuvausta. Tässä prosessissa kaikki transaktiot (sähkö, data, maksuliikenne) kulkevat erilaisten sidosryhmien kautta. Tässä järjestelmässä energiaa tuotetaan keskitetyissä tuotantolaitoksissa ja toimitetaan teollisuus- ja kotikäyttäjille energiayhtiöiden hallinnoimien jakeluverkkojen kautta. Kauppiaat ostavat ja myyvät energiaa pörsseissä ja pankit toimivat maksupalveluntarjoajina hoitaessaan osapuolten tekemiä liiketoimia.

Maksuliikenne kulkee pankkien kaltaisten finanssialan laitosten kautta muun muassa verkko-operaattoreille, energiantuottajille, sekä asukaskuluttajille. Välittäjät ostavat sekä myyvät energiaa, ja pankit toimivat maksujen palveluntarjoajina käsitellen asianomaisten osapuolten liiketapahtumat. Oikealla esitellään Blockchain-järjestelmiin pohjautuva ekosysteemi. Blockchain-pohjaiset energiaprosessit eivät enää vaatisi energiayhtiöitä,

kauppiaita tai pankkeja maksutapahtumissa. Sen sijaan käytettäisiin hajautettua energian-jakelu- ja toimitusjärjestelmää. Tämä järjestelmä käyttäisi Blockchain-pohjaisia älykkäitä sopimuksia ja antaisi kuluttajille mahdollisuuden hallita omia sähköntoimitussopimuksia sekä kulutustietojaan. (Hasse ym. 2016)

Naucler (2017) kertoo Fortumin tekevänsä tutkimusta yhteistyössä ETLA:n (Elinkeinoelämän tutkimuslaitos) kanssa energian jakeluun P2P-verkoston kautta.



Kuva 20. Blockchain ja kotitalouksien energianjakelu Fortumissa (Hasse ym. 2016)

Kuvassa 20 esitellään sitä kuinka Blockchainia voitaisiin hyödyntää energian myynnissä ja jakelussa. Kuvitettuna on asuinyhteisö jaetulla kansallisella sähköverkon tukiasemalla. Tämän takana on lisäksi toinen taso koostuen älymittareista, jotka toimivat osana älykästä sähköverkkoa. (Mattila ym. 2016)

Asuntoyhteisön sähköinfrastruktuuriin voi kuulua kaksi älymittaritasoa. Ensimmäisellä tasolla on yksi älykäs mittari (tai kaksi älykästä mittaria kaksisuuntaiseen mittaukseen) jonka koko asuntoyhteisö jakaa. Toisen tasoon kuuluvat asuntokohtaiset älykkäät mittarit (submeters). Tässä esimerkissä on käytetty Ruotsia, jossa sähkömaksu ja sähköverkkomaksu ovat erillään toisistaan. Yksi idea tämän järjestelyn takana on se, että asukkaat voivat säästää rahaa vähentämällä käytössä olevien verkon käyttöpisteiden määrää. (ETLA 2016.)

Toinen idea on optimoida järjestelmä koko asuntoyhteisön tasolla niin, että yhteisö on mahdollisimman omavarainen ja käyttää verkkoa vain tarvittaessa. Tämän lisäksi verkkoa voidaan käyttää suorittamaan paikallisia markkinoita, jossa sähköä voidaan myydä ja ostaa vertaisverkossa. Tämä rakenne voisi tulevaisuudessa avata asiakkaille pääsyn markkinoille, vaikka heillä ei olisikaan suoraa pääsyä valitsemaan toimittajaa omalle verkkoon kytketylle mittarilleen.
(ETLA 2016.)

Tämän lisäksi Naucler (2017) kertoo myös mahdollisuuksista alueilla urbaanien kaupunkien ulkopuolella, kuten maaseuduilla. Hyvänä esimerkkinä toimii Intia, ja myös Fortumin visio ulottuu sinne asti.

Financial Expressin (2018) artikkelissa puhutaan potentiaalista Intiassa. Tämänhetkisen teknologian kehityksen ansiosta Blockchainin avulla pystytään linkittämään energiateollisuuden laitteita. Näihin laitteisiin kuuluvat esimerkiksi mikroverkot, sähköautot, paristot, sekä jopa biomassalla tuotettu sähkö. Suunnitelmissa on ollut kansallisten sähköverkkojen tuonti alueille, joissa hallitus on jo tarjonnut mikroverkkoja. Tämä on kuitenkin herättänyt vastustusta palveluntarjoajien osalta. Blockchainin avulla tämän kaltaisten alueiden sähkön kulutuskäyttäytymistä ja kirjanpitoa voidaan integroida jo olemassa olevaan kansalliseen sähköverkkoon. Tämä luo alustan Blockchain-pohjaisille sähkömarkkinoille.
(Mobarak, 2018.)

Fortumin kanssa tehdyn haastattelun (Stahl 24.9.2018) perusteella voidaan tehdä seuraava johtopäätös; Blockchain soveltuu parhaiten tilanteisiin, joissa puuttuu ns. luonnollinen tai luotettava kolmas osapuoli kauppojen järjestämiseksi tai takaajaksi. Blockchain toimii esimerkiksi energiakauppojen välisenä markkinana. Blockchainin hyödyt kuitenkin tulevat parhaiten esiin markkinoilla, joissa ei selkeästi ole välittäjää tai muuta osapuolta kaupoille tai varsinaista markkinahintaa sähkölle. Esimerkiksi Pohjoismaissa sähkömarkkina toimii hyvin ja ylijäämäsähkön voi myydä markkinahintaan useammallekin taholle.

Haastattelusta selviää, että Blockchain voi hyvin mahdollistaa ja lisätä uusiutuvien energianlähteiden hyödyntämistä luomalla kauppapaikan uusiutuvan sähkön kysynnän ja tarjonnan kohtaamiseksi. Tästä jo startup-yrityksiä eri puolilla maailmaa. On kuitenkin epätodennäköistä tai aikaista sanoa, että Blockchain voisi merkittävästi tehostaa nykyistä markkinaa Pohjoismaissa, mutta voi mahdollisesti tuoda uudenlaisen kauppapaikan nykyisen rinnalle. (Stahl 24.9.2018.)

Blockchainin suljettu malli voi rajata osallistujia. Avoimessa mallissa taas voi olla haastavaa löytää ansaintalogiikkaa. Regulaatio ja esimerkiksi verotusmalli voi hyvinkin paljon vaikuttaa Blockchainin hyödynnettävyyteen esimerkiksi sillä, miten käsitellään mittarin takana tapahtuvaa kulutusta, onko käytössä netotus tai muu vastaava.
(Stahl 24.9.2018.)

Alla taulukossa on vertailtuna Blockchainien eri muodot ja niiden mahdolliset hyödyt sekä rajoitteet.

Tyyppi	Kuvaus	Hyöty	Rajoite
Julkinen Blockchain	Kaikille osanottajille saatavilla oleva Blockchain-lokikirja	-Avoimuus/läpinäkyvyys -hajautettu malli -muuttumaton (vaikea korruptoida dataa, kun liiketapahtuma kerran toteutettu)	-Suuri määrä osanottajia voi aiheuttaa hitautta -Yksityistietojen avoimuus ei aina hyväksi, esimerkiksi yritysmaailmassa
Suljettu Blockchain	Blockchainin resurssit saatavilla/hallinnoitavissa yrityksen sisäisesti (Rajatut KYC-säännökset pätevät)	-Nopeus (vähemmän osanottajia) -Parempi skaalautuvuus -Sujuvampi konsensusprosessi -Parempi valvonta/säännökset	-Aiheuttaa rajoitteita siihen, kuka voi osallistua verkostoon ja missä määrin

Taulukko 2. Julkisen- sekä suljetun Blockchainin eroavaisuudet.

Stahl (2018) viittaa suljetulla- sekä avoimella mallilla yksityiseen- ja avoimeen Blockchainiin (kappale 2.2.1). Suljetussa mallissa digitaaliset resurssit Blockchainin käyttöön ovat rajoitettu yrityksen/organisaation sisälle rajaten osallistujamäärää. Avoimessa mallissa asia on päinvastainen. Julkinen malli voi olla hyödyllinen, mikäli tavoitteena on suojella käyttäjän anonymiteettiä. Julkisessa mallissa kaikilla osanottajilla on luku- ja kirjoitusoikeudet. Tämän vuoksi avoin lokikirja voi kuitenkin tuoda ongelmia yritykselle. Liiketoiminnassa tulee olla tietynlaista tietoturvaa. Täten liiketoimintadatan jakaminen kaikille osapuolille julkisesti ei ole välttämättä kannattavaa. Tämän takia ehtojen luominen muodostuu

tärkeäksi tekijäksi. Suljetussa Blockchainissa tulisi olla mahdollista kontrolloida sitä kuka pääsee käsiksi mihinkin dataan missäkin olosuhteissa. Taulukossa 21 viitataan sujuvampaan konsensusprosessiin suljetun Blockchainin hyötynä. Tällä tarkoitetaan sitä, että yksityisessä Blockchainissa on suljetun luonteensa vuoksi vähemmän osanottajia (solmuja). Täten yleensä konsensusalgoritmi voi olla eri kuin julkisessa Blockchainissa. Yksityisessä voi olla käytössä BFT eli Byzantine Fault Tolerance (kappale 2.1). Julkisessa Blockchainissa on sen sijaan usein käytössä Proof-Of-Work (kappale 2.2.3) tai vastaava.

Tämän perusteella voidaan tehdä useampia havaintoja. Suljetun mallin Blockchainia voidaan käyttää optimaalisesti tilanteissa, joissa sidosryhmien välisessä kanssakäymisessä halutaan pitää liiketapahtuman sopimuksen sisällön (esimerkiksi maksettu hinta) yksityisenä. Vain asianomaiset osapuolet voivat tarkastella sopimuksen yksityiskohtia. Sama pätee myös muiden osapuolten kanssa suoritettuihin tapahtumiin.

Hyöty	Julkinen/suljettu	Hyödyn taso: EV	Hyödyn taso: Sähkö
Maksuliikenteen yksinkertaistaminen	Julkinen, P2P	Korkea	Korkea
Luottamus sidosryhmien välillä	Julkinen	Korkea	Korkea
Läpinäkyvyys	Julkinen & Suljettu	Keskitaso	Keskitaso
Anonymiteetti	Julkinen	Keskitaso	Keskitaso
Suoritusteho	Julkinen	Alhainen	Alhainen
Skaalautuvuus	Julkinen	Alhainen	Alhainen
Taloudelliset säästöt toimintakuluissa	Julkinen	Korkea	Keskitaso

Taulukko 3. Blockchainin eri hyödyt ja niiden taso valituissa käyttötapauksissa taulukoinnin muodossa.

Ylläolevassa taulukossa vertaillaan kerätyn datan perusteella julkisen sekä suljetun/rajoitetun Blockchain-alustan hyötyjä tutkituissa käyttötapauksissa. Usein puhuttaessa Blockchainin käyttötapauksista energiateollisuudessa viitataan julkiseen Blockchainiin. Tähän on muutamia tärkeitä syitä.

Julkisessa Blockchainissa kaikki osanottajat voivat tehdä kauppaa ilman että heidän tarvitse pyytää lupaa verkkoon osallistumiseen. Energiateollisuudessa tapahtuu laajamittainen muutos kohti järjestelmää, jossa miljardit laitteet voivat tasapainottaa sähköverkkoa

suurten keskitettyjen voimalaitosten sijasta. Tällaisilla aloilla laaja-alainen yhteentoimivuus on erittäin tärkeää.

Sähköautot ovat hyvä esimerkki. Nykyisen latausinfrastruktuurin avulla pystytään yleisesti tukemaan tiellä noin viisi miljoonaa sähköautoa. Kyseinen infrastruktuuri on kuitenkin suurelta osin heikosti rakennettu, mikä taas johtaa erittäin alhaiseen omaisuuden käyttöön ja konfliktialttiiseen asiakaskokemukseen (kuten pakollinen tarve käyttää erilaisia valtuustietoja erilaisille veloitusverkoille). Kun siirrytään tien päästä viidestä miljoonasta 50:een tai jopa 500 miljoonaan sähköautoon, tämä liiketoimintatapa ei yksinkertaisesti ole skaalautuva. (Morris, Hartnett, 2019.)

Tavoitteena on digitaalinen infrastruktuuri, joka antaa jokaiselle sähköautolle ja latausasemalle mahdollisuuden toimia latausverkoston solmuna – riippumatta siitä kuka sitä ylläpitää tai operoi – toimien automaattisesti vertaisverkossa. Tämän saavuttamiseksi tarvitsemme menetelmän, jolla sähköautojen lataustapahtumien tiedot jaetaan useille sidosryhmille. Kappaleessa on kuitenkin mainittu jo aiemmin, että tämä voi olla hyvin haasteellista sidosryhmien paljouden vuoksi. (Morris, Hartnett, 2019.)

Tässä julkiset Blockchainit pääsevät loistamaan; käyttäessään julkista verkkoa mikään yksittäinen entiteetti ei ole vastuussa mistään liiketapahtumasta tai sen tai toimeenpanosta. Tässä sidosryhmien ekosysteemissä millään keskitetyllä osapuolella ei myöskään ole yksinoikeutta dataan. (Morris, Hartnett, 2019.)

Perinteiset keskitetyt IoT-alustat ja yksityiset Blockchainit pystyvät suorittamaan monimutkaisia liiketapahtumia. Toinen haaste on kuitenkin saada suuri joukko osapuolia digitalisoitumaan keskitetysti hallittujen sääntöjen avulla. Nämä osapuolet pitäisi vielä saada luottamaan yksittäiseen ratkaisuntoimittajaan yksityisen Blockchain-verkon ylläpitämisessä ja tapahtumien täyttöön panossa. (Morris, Hartnett, 2019.)

Maksuliikenteen yksinkertaistamisessa julkinen vertaisverkossa toimiva Blockchain on hyödyllinen sekä sähköautojen latausinfrastruktuurissa että energianjakelussa. Sidosryhmien välinen luottamus on avainasemassa ja sitä voidaan parantaa Blockchainin avulla. Kuten ylempänä on kuitenkin mainittu, avoin lokikirja ei välttämättä ole paras vaihtoehto yritystoiminnan kuluttajasuojan kannalta.

Tässä tapauksessa niin sanottu hybridi ”permissioned” (luvanvarainen) -mallinen Blockchain voi olla parempi vaihtoehto. Frankenfieldin (2019) kirjoittaman artikkelin mukaan tämä rajoitettu malli eroaa yksityisestä Blockchainista tietyssä määrin. Yksityisessä

Blockchainissa vain tunnetut tai sallitut osanottajat voivat osallistua verkostoon. Permissioned-mallinen Blockchain voi sallia kenen tahansa osallistua verkkoon, kunhan osanottajan rooli ja identiteetti saadaan vahvistettua ja määriteltyä.

Taulukossa 22 mainitaan hyötysuhteen vertailukohteina myös suoritusteho sekä skaalautuvuus. Tämänhetkisten julkisten Blockchainien tunnettu haaste on niiden rajoitettu suorituskyky. Tällä tarkoitetaan esimerkiksi sitä, että kuinka monta transaktiota voidaan suorittaa sekunnissa. Tämä rajoitettu suorituskyky taas vaikuttaa suoraan siihen, miten nämä Blockchain-pohjaiset sovellukset kykenevät skaalautumaan. Tämä aihealue on aktiivisen tutkimuksen kohteena ja toistaiseksi haasteita riittää.

Stahl (2018) mainitsee haastattelussaan myös Blockchainin mahdollisina haasteina hitauden, mikäli mukana on paljon transaktioita. Lisäksi tarvittava muistikapasiteetti sekä liiketoimintamalli aiheuttavat haasteita. Kappaleessa 2.1.4 puhutaan Blockchainin tuomista haasteista. Kappaleessa mainitaan suorituskyky eräänä kriittisenä haasteena Blockchainille. Mikäli useita tapahtumia suoritetaan samanaikaisesti, voi Blockchainin prosessointiteho jäädä vajavaiseksi. Tämä voi aiheuttaa vakavia ongelmia luotettavuuden kanssa. Haastattelun pohjalta kerätyt epäkohdat korreloivat kappaleessa 2.1.4:ssa lueteltujen haasteiden kanssa. Täten voidaan todeta, että Blockchainin standardit energiateollisuudessa eivät vielä tässä vaiheessa ole vaaditulla tasolla optimaalista käyttöönottoa varten. Kaiken kaikkiaan haastattelun pohjalta voidaan todeta, että vaikka Blockchain on tutkimuksen kohteena ja pilotointeja on useita erilaisia, on se teknologiana vielä haasteellinen.

Saatujen tietojen perusteella voidaan sanoa, että Blockchain ei ole vielä syrjäyttämässä perinteisiä toimintamalleja. Kuitenkin pilotointeja ja hankkeita useampia, ja käyttömahdollisuuksia tutkitaan laajasti. Haastattelun pohjalta saadun datan pohjalta voidaan sanoa, että muun muassa yllä mainittujen onnistuneiden pilotointien vuoksi hyvinkin käytännöllisiä käyttökohteita ollaan harkitsemassa tulevaisuudelle. Kysymyksenä herää kuitenkin kannattavuus ja muun muassa ansaintalogiikka. Monissa osa-alueissa on vielä haasteita ja tutkimustyö on jatkuvassa tilassa. Lisäksi Blockchainin ja energiateollisuuden integraatiota varten tarvitaan muutoksia lakisäännöksiin, vaatimuksiin ja standardeihin. Näiden ylitse pääseminen voi olla haasteellista ja aikaa vievää. Oikeudelliset- ja sääntelypuitteet on vielä suunniteltava vastaamaan hajautettujen liiketoimintamallien vaatimuksia ja tarjoamaan suojaa energiankuluttajille. Muutokseen menevästä ajasta ei voida sanoa varmuudella mitään. Toistaiseksi Blockchain ei ole kuitenkaan löydösten perusteella syrjäyttämässä vallitsevia järjestelmiä, ja muutosvaihe on hidas. Sen sijaan se voi toimia hyötyjä tuovana tukevana työkaluna jo vallitseville menetelmille.

4 Pohdinta ja johtopäätökset

Tutkimuksessa käytiin läpi lohkoketjuteknologiaa ja sen eri osa-alueita mahdollisimman kattavasti ja objektiivisesti. Tutkimus aloitettiin tietoperustasta ja lopuksi käytiin läpi käyttötapauksia energiateollisuuden alalta. Pääasiallisena tutkimuskohteena oli energiayritys Fortumin Blockchainiin perustuvat käyttötapaukset. Tutkimus suoritettiin luonteensa vuoksi eksploratiivisena. Lisäksi empiiristä materiaalia pyrittiin käyttämään aina mahdollisuuksien puitteissa.

Kappale kaksi aloitettiin niin sanotulla yleisteorialla, jossa pyrittiin avaamaan Blockchainia lukijalle yleismaailmallisella tasolla. Tähän kappaleeseen sisältyivät muun muassa Blockchainin historia, käyttötarkoitus, liittyvät konseptit ynnä muu vastaava. Tämän lisäksi kappaleessa käytiin läpi yksityiskohtaisempaa, tutkimusaiheeseen liittyen relevanttia teoriaa. Tätä kappaletta kutsuttiin nimellä käsiteanalyysi.

Kappaleesta kaksi selvisi, että Blockchain on avoin ja autonominen vertaisverkossa toimiva hajautettu digitaalinen lokikirjajärjestelmä, jota voidaan käyttää muun muassa liiketapahtumien säilömiseen tietoturvallisesti ja läpinäkyvästi. Kun data on kirjoitettu Blockchainiin, kaikki tietoverkon osanottajat saavat kopion lohkosta ja voivat tarkastella dataa avoimesti julkisen avaimen voimin. Blockchain toimii perinteisen client-server -toimintamallin sijasta P2P (Peer-to-Peer) -vertaisverkossa, ilman keskinäistä auktoriteettia. Tämä tarkoittaa sitä, että esimerkiksi liiketapahtumissa pankin tai muun kolmannen osapuolen sijasta luodaan konsensusta kolmen kryptografisen menetelmän voimin.

Ensimmäisenä tietoturvamenetelmänä käytetään digitaalisia allekirjoituksia luomalla avainpari. Tällä toteutetaan lohkon sisällön salaus ja purkaus asianomaisten kesken. Lisäksi allekirjoituksia käytetään verifikaation muotona. Toisena menetelmänä käytetään hajautusalgoritmeja datan tiivistämiseen. Jokainen lohko sisältää oman sekä edellisen lohkon hajautustiivisteen. Blockchain käyttää näitä hajautustiivisteitä kiinnittämään lohkot toisiinsa kronologisessa järjestyksessä, luoden täten lohkoketjun. Viimeisenä menetelmänä tietoverkon solmut kommunikoivat keskenään vertaisverkossa ja luovat konsensusta käyttäen Proof-Of-Work -protokollaa.

Kappaleessa käytiin myös läpi Blockchain tuomia mahdollisuuksia teollisen internetin sekä muun muassa älykkäiden sopimusten näkökulmasta. Yritysten kiinnostus ja investointi IoT- sekä Blockchain-pohjaisiin ratkaisuihin on kasvussa, luoden uusia mahdollisuuksia. Kappaleesta selvisi, että oikein toteutettuna Blockchain voi parantaa teollisen internetin

skaalautuvuutta, tietoturvaa sekä luotettavuutta. Käytättämällä keskitetyn ekosysteemin sijasta hajautettua Blockchainia hyödyntävää mallia voidaan tuottaa huomattavia taloudellisia säästöjä. Blockchainilla on täten selkeästi potentiaalia parantaa teollisen internetin monia eri osa-alueita. Kuitenkin tutkimuksen pohjalta voidaan myös nähdä, että Blockchainilla on oman haasteensa. Näihin haasteisiin kuuluvat esimerkiksi standardointi, tietotaidon puute sekä lainopilliset haasteet. Vaikka teknologiana se on digitaalisen maailman mittakaavassa uusi, on ihmisten tietoisuus Blockchainista selkeästi kasvussa. Tällä hetkellä on vaikea kuitenkaan antaa selkeää vastausta teollisen internetin ja Blockchainin mahdollisen integraation tulevaisuudesta. Potentiaalia selkeästi löytyy, mutta vastuu jatkokehittämisestä jää teknologiayhteisön käsiin.

Kappaleen kaksi pohjalta voidaan todeta, että Blockchain on teknisesti haastava kokonaisuus sisältäen paljon muuttujia. Jopa sen pintapuolinen ymmärrys vaatii perehtymistä ja jatkuvaa itsenäistä tutkimustyötä. Byzantine Generals Problem, Hashcash, Bitcoin, sekä muut vastaavat teoriat ja konseptit ovat luoneet pohjaa nykypäivän Blockchainille. Alun perin julkiseksi lokikirjaksi suunniteltu järjestelmä on aikojen saatossa saanut uusia muotoja. Yksityiset sekä konsortiomuotoiset Blockchainit tuovat yhteensopivuutta liiketoiminnan maailmaan ja yritysmaailmassa tärkeään yksityisyyden parantamiseen. Lisäksi saavutetaan kaikille osapuolille voitollista kulujen leikkausta.

Kappaleessa kolme käytiin läpi tutkimustapauksia eli Blockchainin hyötyjä energiateollisuudessa. Kappaleessa vastataan myös tutkimuskysymykseen. Tutkimuksessa pyrittiin selvittämään, voidaanko Blockchainia hyödyntää energiateollisuudessa. Tähän jatkettiin vielä tutkimalla käyttötapauksia erityisesti Fortumin kaltaisen energiayhtiön näkökulmasta. Haettuja vastauksia saatiin verkko- sekä kirjamateriaalin lisäksi haastattelemalla alan ammattilaisia. Tutkimuksen haastattelun kohteena oli Suomalainen energiayhtiö Fortum. Fortum on jo jonkin aikaa investoinut aikaa ja resursseja Blockchainin tutkimukseen. Fortumilla on useita kasvuprojekteja, joihin kuuluu myös Blockchain. Tämän tutkimusosaston johtajana toimii suomessa Riitta Stahl. Olimme yhteydessä häneen ja saimme avattua monia asioita liittyen energiatuotantoon ja Blockchainin tuomiin mahdollisuuksiin. Fortum on ollut tiiviissä yhteistyössä ETLA:n (Elinkeinoelämän tutkimuslaitos) kanssa. Heidän yhteisenä tavoitteenaan on ollut muodostaa ymmärrystä Blockchainin ja sen eri liiketoimintamahdollisuuksien ympärille Suomessa.

Saatujen vastauksien perusteella voidaan vastata tutkimuskysymykseen. Blockchainia voidaan käyttää tukena energiateollisuudessa ja sen kehityksessä. Fortum tapauksessa pilotoituja käyttötapauksia on useita. Tässä tutkimuksessa käytiin läpi kuitenkin vain kahta olennaisiksi koettua käyttötapausta. Valitut käyttötapaukset olivat Blockchainin hyödyntä-

minen sähköautoilun (EV) latausinfrastuktuurissa, sekä lisäksi energianjakelu hyödyntäen Blockchainia. Tutkimuksesta selviää, että vaikka Blockchain on nouseva nimi energiateollisuuden maailmassa, on se vielä hyvin pitkälti tutkimusvaiheessa. Pilotointeja on muutamia ja osa niistä hyvinkin sovellettavia mahdollisuuksia. Muun muassa Blockchainin integraatiota sähköautoiluun on pilotoitu suhteellisen kattavasti, toistaiseksi onnistunein tuloksin. Fortum on osallistunut useaan pilottiin, muun muassa Oslo2Rome, sekä Share&Charge. Blockchainia voidaan käyttää luomaan hajautettu ekosysteemi kaikkien sähköautoilun infrastruktuuriin kuuluvien osapuolten välille. Tämä tarkoittaa myös roamingmaksujen poistamista Euroopassa sallien sähköautojen latauksen eri maissa ilman kolmansien osapuolien lisäkustannuksia. Lisäksi Blockchainilla voidaan positiivisesti tuoda esille sähköautoilun etuja ja mahdollisesti leikata hallinnollisia kuluja älykkäillä sopimuksilla.

Toisena tämän työn tutkimuskohteena oli energianjakelu vertaisverkostossa käyttäen Blockchain-alustaa. Tässä käyttötapauksessa Blockchainia voidaan käyttää hyväksi esimerkiksi ylijäämäsähkön markkinapaikan luomiseksi. Hajautettu alusta poistaa tarpeen kolmannelle osapuolelle. Tutkimuksen mukaan paras tai luontainen käyttötapaus Blockchainille on markkinoilla, jossa puuttuu luonnollinen/luotettava kolmas osapuoli kauppojen järjestämiseksi tai takaajaksi. Blockchain toimii esimerkiksi energiakauppojen välisenä markkinana. Blockchainin hyödyt tulevat kuitenkin parhaiten esiin markkinoilla, joissa ei selkeästi ole välittäjää tai muuta osapuolta kaupoille tai varsinaista markkinahintaa sähkölle.

Tutkimuksen löydösten perusteella selvisi myös, ettei mahdollinen energiateollisuuden Blockchainin integraatio ole haasteeton. Mahdollinen hitaus, vaadittu muistikapasiteetti ja liiketoimintamalli voivat olla suuria haasteita Blockchainin tuomisessa energiateollisuuden tukipilariksi. Vaikka potentiaalia on olemassa ja Blockchainin integraatio on todettu toimivaksi tietyissä käyttötapauksissa, on nämä haasteet silti tunnistettava. Kappaleen pohjalta voidaan päätyä siihen päätelmään, että vaikka Blockchain energiateollisuuden maailmassa on yhä tutkimusvaiheessa, on se silti hyvin varteenotettava tukipilari jo olemassa oleville teknologioille. Tämä mahdollistaa erilaisia sekä kuluttajille että tuottajille etua tuovia toiminnallisuuksia. Tutkimuksen loppupäätelmänä voidaan sanoa, että Blockchain on vielä suhteellisen uusi ja nouseva konsepti, jolla on potentiaalia tehdä muutosta eri teollisuuden aloilla. Sitä kuitenkin ympäröi skeptisyyden ja epäkypsyyden ilmapiiri. Sen popularisointiin tulee menemään aikaa. Yrityksille, jotka haluavat hyödyntää Blockchainia on paljon vaihtoehtoja tarjolla. Tutkijan roolissa on kuitenkin objektiivisuus tärkeää, ja täten mainittava haasteiden painoarvo. Digitaalinen aikakausi mahdollista erilaisten teknologioiden integraation, ja perinteiset toimintamallit ovat usein ottaneet osumaa tämän muutosvaiheen

aikana. Mikäli Blockchain halutaan ottaa käyttöön onnistuneesti, tarvitaan muutakin kuin pelkkiä ohjelmoijia ja insinöörejä. Työvoimassa ja henkilöstössä tulee olemaan muutoksia. Perinteisiä työnimikkeitä tullaan mahdollisesti korvaamaan uusilla. Tämä muutos ei ole kaikkien mieleen. Blockchainin tai vaikkapa koneoppimisen kaltaiset modernit nousevat teknologiat vaativat perinteisten toimialojen henkilöstön tietotaidon nostamista. Matka on vielä pitkä ja emme voi sanoa tarkalleen mikä on lopputavoite tai kauan sen saavuttamiseen menee. On vaikea edes määritellä muutoksen tarpeellisuutta. Tutkimuksen kannalta voidaan kuitenkin todeta, että Blockchainia voidaan käyttää tukipilarina energiateollisuudessa. Se voi tuoda ratkaisuja monien eri alojen haasteisiin, ja energiateollisuus on ehdottomasti yksi näistä aloista.

Digitaalisessa maailmassa käytetään usein termejä ”disruptive” eli perinteisiin menetelmiin häiriötä aiheuttava, sekä ”foundational” eli perustava, viitaten uusiin nouseviin teknologioihin. Blockchainin maailmassa kiistellään siitä, kumpi näistä termeistä voidaan yhdistää Blockchainiin. Ensimmäisellä viitataan siihen, että Blockchain korvaa tai luo uuden järjestelmän täysin. Muutos on verrattavissa esimerkiksi Tim Berners-Leen World Wide Webiin. Toinen taas viittaa siihen, että Blockchain tulee hiljaisesti taustalla tukemaan jo olemassa olevia teknologioita ja prosesseja tehden niistä kannattavampia kaikille osapuolille. Tämä muutos on hidasta ja voi kestää vuosikymmeniä. Tutkimuksen pohjalta päädytään siihen, että Blockchain on niin kutsuttu ”foundational technology” eli se vaatii aikaa kypsyäkseen teknologiana. Suurta huomattavaa muutosta ei mitä luultavammin tulla näkemään lyhyessä aikavälissä. Sen sijaan pitkässä aikavälissä suuria muutoksia voi tapahtua.

Teoksen tarkoituksena on antaa yleinen katsaus Blockchainin maailmaan ja levittää tietoisuutta sen mahdollisesta arvosta, eritoten energiateollisuuden alalla. Toivon, että tätä teosta käytettään jatkotutkimuksen työkaluna. Toivon mukaan kaikki Blockchainista kiinnostuneet saavat teoksen luettuaan muodostettua perustasoa syvällisempää ymmärrystä aiheesta ja sen relevanssista. Toivon mukaan teos herättää lukijassa erinäisiä ajatuksia ja mahdollisesti toimii inspiraation lähteenä. Jokainen voi lukemansa perusteella muodostaa Blockchainista oman mielipiteensä. Ratkaisevaa oikeata tai väärää vastausta tuskin on olemassa.

Lähteet

Accenture 2018. Blockchain Technology. How banks are building a real-time global payment network. Accenture Mobility. Saatavilla: https://www.accenture.com/t20181009T020401Z__w__/us-en/_acnmedia/PDF-35/Accenture-Blockchain-How-Banks-Building-Real-Time-Global-Payment-Network.pdf. Luettu: 10.10.2018.

Aida Service 2017. What is a smart contract and how does it work in our AIDA service. Medium. Luettavissa: https://medium.com/@aidaservice/what-is-a-smart-contract-and-how-does-it-work-in-our-aida-service-a7d7a2a6eeaa. Luettu: 17.5.2018.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A. 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Luettavissa: https://www.sciencedirect.com/science/article/pii/S1364032118307184. Luettu: 16.9.2019

Au, S. 2018. If you understand Hash Functions, you'll understand Blockchains. Decentralize Today. Luettavissa: https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d. Luettu: 11.10.2018.

Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. Luettavissa: http://www.hashcash.org/papers/hashcash.pdf. Luettu: 15.10.2018.

Bambara, J., Allen, P. 2018. Blockchain: A practical guide to developing business, law, and technology solutions. McGraw & Hill Education. New York.

Banafa, A. 2018. The Blockchain Wave in 2019 and Beyond. Medium. Saatavilla: https://medium.com/@banafa/the-blockchain-wave-in-2019-and-beyond-9f70152bef6. Luettu: 18.11.2018.

Banafa, A. 2017. IoT and Blockchain Convergence: Benefits and Challenges. IEEE. Luettavissa: https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html. Luettu: 5.9.2018.

Bashir, I. 2017. Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained. Packt Publishing. Birmingham.

Buterin, V. 2015. A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. Luettavissa: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Luettu 1.5.2018.

Buterin, V. 2017. The Meaning of Decentralization. Medium. Luettavissa: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Luettu: 17.4.2018.

Cheng, R. & Song, D. 2018. Smart Contracts. Luettavissa: https://berkeley-blockchain.github.io/cs294-144-s18/assets/docs/02-smartcontracts-jan-29-2018-v2.pdf. Luettu: 20.4.2018.

Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. 2016. Blockchain technology: Beyond bitcoin. Applied Innovation Review. 2nd ed. Berkeley: Sutardja Center for Entrepreneurship & Technology, University of Berkeley, California, pp.6-19. Luettavissa: http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf. Luettu: 28. maaliskuuta 2018.

Deloitte 2018. 2018 Global Blockchain Survey. Luettavissa: https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html. Luettu: 5.9.2018.

Demary, M. & Demary, V. 2017. Financial Technology: Blockchain - Down to Earth. Cologne Institute for Economic Research (IW), Cologne. Luettavissa: https://www.econstor.eu/bitstream/10419/157589/1/IW-Kurzbericht_2017-02.pdf. Luettu: 1.7.2018.

De Vries, A. 2018. Bitcoin's Growing Energy Problem. Joule. Luettavissa: https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6. Luettu: 16.10.2018.

Dudovskiy, J. 2019. Exploratory Research - Research Methodology. Research-methodology.net. Luettavissa: https://research-methodology.net/research-methodology/research-design/exploratory-research/. Luettu: 24.11.2019.

Etla 2016. Blockchains Boosting Finnish industry (BOND). Luettavissa: https://www.etla.fi/tutkimukset/blockchains-bond/. Luettu: 5.11.2018.

FE Bureau 2018. Chaining the energy: Blockchain may bring changes in the energy industry. The Financial Express. Saatavilla: https://www.financialexpress.com/opinion/chaining-the-energy-blockchain-may-bring-changes-in-the-energy-industry/1189140/. Luettu: 10.10.2018.

Feng, X., Yang T. L., Wang, L. & Vinel, A. 2012. Internet of Things. International Journal of Communication Systems. Wiley Online Library. Luettavissa: https://s3.amazonaws.com/academia.edu.documents/36946966/danainfo.acppwiszgmk2n0u279qu76contentserver.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1536857076&Signature=07VFU1DQi4VAv5oxPidQo2ByP4U%3D&response-content-disposition=inline%3B%20filename%3DInternet_of_Things.pdf. Luettu: 10.9.2018.

Frankenfield, J. 2019. Permissioned Blockchains. Investopedia. Luettavissa: https://www.investopedia.com/terms/p/permissioned-blockchains.asp. Luettu: 8.10.2019.

Gartner 2018. Internet of Things. Luettavissa: https://www.gartner.com/it-glossary/internet-of-things/. Luettu: 10.9.2018.

Gorenflo, C., Golab, L. & Keshav, S. (2019). Mitigating Trust Issues in Electric Vehicle Charging using a Blockchain. Luettavissa: https://www.sciencedaily.com/releases/2019/08/190814144501.htm. Luettu: 21.9.2019.

Hallamaa, T. 2018. Lohkoketjut demokratisoivat internetin ja mullistavat maailman – mutta huomaammeko mitään? Yle. Luettavissa: https://yle.fi/uutiset/3-10027239. Luettu: 1.9.2018.

Hasse, F., von Perfall, A., Hillebrand, T., Smole, E., Lay, L. & Charlet, M. (2016). Blockchain – an opportunity for energy producers and consumers? PwC Global power & utilities. Luettavissa: https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf. Luettu: 19.10.2018.

Hessekiel, D. 2018. The Future Of Social Impact Is...Blockchain. Forbes. Luettavissa: https://www.forbes.com/sites/davidhessekiel/2018/04/03/the-future-of-social-impact-is-blockchain/#3eee861c3fdd. Luettu: 10.6.2018.

IBM 2016. Watson IoT and Blockchain: Distruptor and game changer. Build trust, reduce costs, and accelerate transactions. IBM Watson IoT. Luettavissa:

https://public.dhe.ibm.com/common/ssi/ecm/ww/en/ww912350usen/watson-iot-cognitive-solutions-ww-infographic-general-ww912350usen-20180306.pdf. Luettu: 1.11.2018.

IBM 2014. Z/OS Cryptographic Services ICSF Overview. Luettavissa: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.csfb500/csfb5za251.html. Luettu: 11.101.2018.

I-Scoop 2018. Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge. Luettavissa: https://www.i-scoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/. Luettu: 28.11.2018.

Jscrambler 2016. Hashing Algorithms. Luettavissa: https://blog.jscrambler.com/hashing-algorithms/. Luettu: 11.10.2018.

Konstantopoulos, G. 2018. Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake. Medium. Luettavissa: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb. Luettu: 15.10.2018.

Krawisz, D. 2013. The Proof-of-Work Concept. Satoshi Nakamoto Institute. Luettavissa: http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/. Luettu: 28.3.2018.

Lamport, L., Shostak, R. & Pease, M. (1982). The Byzantine Generals problem. Luettavissa: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf. Luettu: 1.6.2018.

Lehmusvirta, A. 2018. Lohkoketjut voivat tehdä pankeista ja pörsseistä turhia: nämä kaikki yhtiöt ovat jo vauhdissa. Tivi. Saatavilla: https://www.tivi.fi/Kaikki_uutiset/lohkoketjut-voivat-tehda-pankeista-ja-porsseista-turhia-nama-kaikki-yhtiot-ovat-jo-vauhdissa-6681441. Luettu: 10.10.2018.

Lewis, A. 2015. A Gentle Introduction to Blockchain Technology. Brave New Coin. Luettavissa: https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf. Luettu: 10.6.2018.

Manyika, J., Chui, M., Bughlin, J., Dobbs, R., Bisson, P. & Marrs, A. 2013. Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey & Company. Luettavissa: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies. Luettu: 4.4.2018.

Mapo, 2018. Comprehensive List of Banks using Blockchain Technology. Hacker Noon. Medium. Luettavissa: https://hackernoon.com/comprehensive-list-of-banks-using-blockchain-technology-97c08fa88385. Luettu: 17.10.2018.

Mattila, J., Seppälä, T., Naucler, C., Stahl, R., Tikkanen, M., Bådenlid, A. & Seppälä, J. (2016). Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry. No. 43. ETLA. Luettavissa: https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-43.pdf. Luettu: 24.9.2018.

Maverick, J.B. 2018. The Difference between a nostro and vostro account. Investopedia. Saatavilla: https://www.investopedia.com/ask/answers/051815/what-difference-between-nostro-and-vostro-account.asp. Luettu: 13.11.2018.

Morgan, J. 2014. A Simple Explanation of 'The Internet of Things'. Forbes. Luettavissa: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#5cc7aa751d09. Luettu: 9.9.2018.

Morris, J. & Hartnett, S. 2019. The argument for public blockchains in the energy sector. GreenBiz. Luettavissa: https://www.greenbiz.com/article/argument-public-blockchains-energy-sector. Luettu: 9.10.2019.

Mougayar, W. 2016. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons, Inc. Hoboken, New Jersey.

Myerson, R. 1997. Game Theory: Analysis of Conflict. Harvard University Press. Cumberland.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. Luettavissa: https://bitcoin.org/bitcoin.pdf. Luettu: 1.4.2018.

Naucler, C. 2017. How can Blockchain change the energy market. Fortum. Luettavissa: https://energia.fi/files/2307/Naucler_Catarina_How_can_Blockchain_change_the_energy_market.pdf. Luettu: 15.6.2018.

Newman, P. 2018. IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers. Business Insider. Luettavissa:

https://www.businessinsider.com/internet-of-things-report?r=US&IR=T&IR=T. Luettu: 10.9.2018.

Nohe, P. 2018. The difference between Encryption, Hashing and Salting. Hashed Out. Luettavissa: https://www.thesslstore.com/blog/difference-encryption-hashing-salting/. Luettu: 11.10.2018.

Panetta, K. 2018. 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018. Gartner. Luettavissa: https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/. Luettu: 7.9.2018.

Pwc 2017. Redrawing the lines: FinTech's growing influence on Financial Services. Luettavissa: https://www.pwc.com/jg/en/publications/pwc-global-fintech-report-17.3.17-final.pdf. Luettu: 18.11.2018.

Scott-Briggs, A. 2018. Who Invented Blockchain Technology? TechBullion. Luettavissa: https://www.techbullion.com/invented-blockchain-technology/. Luettu: 3.4.2018.

Share&Charge 2018. Share&Charge - Oslo2Rome-Initiative. Luettavissa: https://shareandcharge.com/oslo-2-rome/. Luettu: 6.11.2018.

Simpson, I. 2018. To Understand Blockchains, You Should Understand Cryptographic Hashes First. Medium. Luettavissa: https://medium.com/vandal-press/to-understand-blockchains-you-should-understand-cryptographic-hashes-first-for-normies-93bc7645e816. Luettu: 11.10.2018.

Soisalon-Soininen, J. 2018. Lohkoketjut ja algoritmit muuttavat pian asuntokaupan ja rahaliikenteen, Nordean von Koskull sanoo – maailma on hyvin herkässä tilassa, siitä kertoo neljä keskeistä paradoksia. Kauppalehti.fi. Luettavissa: https://www.kauppalehti.fi/uutiset/lohkoketjut-ja-algoritmit-muuttavat-pian-asuntokaupan-ja-rahaliikenteen-nordean-von-koskull-sanoo-maailma-on-hyvin-herkassa-tilassa-siita-kertoo-nelja-keskeista-paradoksia/a737cd5e-2404-38a8-a61b-eef5b5f7336b. Luettu: 13.11.2018.

Stahl, R. 24.9.2018. Manager, Growth Projects. Fortum Oyj, Corporate Center. Haastattelu. Espoo.

Szabo, N. 1996. Smart Contracts: Building Blocks for Digital Markets. Alamut. Luettavissa: http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html. Luettu: 4.4.2018.

Tapscott, D. & Tapscott, A. 2016. Blockchain revolution. Penguin Books Ltd. New York.

Thake, M. 2018. What is Proof-of-Work (PoW)? – nakamo.to. Medium. Luettavissa: https://medium.com/nakamo-to/what-is-proof-of-work-pow-2574ddebf916. Luettu: 15.10.2018.

The Internet of Things 2019. IoT Smart City – What is Smart Home? • The Internet of Things. [online] Available at: http://www.infiniteinformationtechnology.com/iot-smart-city-what-is-smart-home [Accessed 12 Sep. 2019].

Tozzi, C. 2017. Byzantine Fault Tolerance: The Key for Blockchains. NASDAQ. Luettavissa: https://www.nasdaq.com/article/byzantine-fault-tolerance-the-key-for-blockchains-cm810058. Luettu: 1.4.2018.
University of Waterloo 2019. Researchers use blockchain to drive electric-vehicle infrastructure. ScienceDaily. Luettavissa: www.sciencedaily.com/releases/2019/08/190814144501.htm. Luettu: 12.9.2019.

Vaidya, K. 2016. The Byzantine Generals' Problem – All Things Ledger. Medium. Luettavissa: https://medium.com/all-things-ledger/the-byzantine-generals-problem-168553f31480. Luettu: 17.4.2018.

Van Der Meulen, R. 2017. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Gartner. Luettavissa: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. Luettu: 8.9.2018.

Virtanen, J. 2018. Nordea lähtee mukaan lohkoketjubisnekseen – perustajajäseneksi ensimmäiseen trade finance -järjestelmään. Tivi. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/nordea-lahtee-mukaan-lohkoketjubisnekseen-perustajajaseneksi-ensimmaiseen-trade-finance-jarjestelmaan-6690784. Luettu: 10.10.2018.

Yin, R. 2014. Case study research: design and methods. 5th edition. Sage Publication. London.