Tampereen yliopisto

Jarkko Nopanen

LOHKOKETJUN HYÖDYNTÄMINEN KOHDEYRITYKSEN TUOTANTOKETJUSSA

Tekniikan ja luonnontieteiden tiedekunta
Kandidaatintyö
Maaliskuu 2019

TIIVISTELMÄ

Jarkko Nopanen: Lohkoketjun hyödyntäminen kohdeyrityksen tuotantoketjussa
Tampereen teknillinen yliopisto
Kandidaatintyö, 27 sivua
Maaliskuu 2019
Teknisten tieteiden TkK-tutkinto-ohjelma
Pääaine: Automaatiotekniikka
Tarkastaja: Yliopisto-opettaja Mikko Salmenperä

Avainsanat: lohkoketju, lohkoketjuteknologia, vertaisverkko, hajautettu systeemi, toimitusketju, tuotantoketju

Lohkoketjuteknologia ei ole vielä yleisesti käytössä virtuaalivaluuttojen ulkopuolella monissa yrityksissä, mutta lohkoketjulle on jo kehitetty muitakin sovelluskohteita. Kohdeyritys haluaa selvittää lohkoketjun hyödyntämismahdollisuuksia tuotantoketjussaan. Lohkoketjun avulla perinteinen keskitetty järjestelmä voidaan muuttaa hajautetuksi, ja parantaa tuotantoketjun läpinäkyvyyttä sekä tuotteiden jäljittämistä. Lohkoketjuun tallennetut tiedot pysyvät muuttumattomina, ja kaikkien tapahtuneiden transaktioiden historiatietoja voidaan tarkastella. Tässä kandidaatintyössä esitellään lohkoketjuteknologia, kohdeyrityksen tuotantoketju ja ehdotus lohkoketjun hyödyntämiselle kohdeyrityksessä.

ALKUSANAT

Aluksi haluaisin kiittää Jani Savinaista todella mielenkiintoisesta työn aiheesta ja kaikesta avusta ja tiedoista työn eri vaiheissa. Ilman hänen apuaan en olisi luultavasti päätynyt tutustumaan lohkoketjuteknologiaan, ja ymmärtämään sen tarjoamia mahdollisuuksia näin tarkalla tasolla.

” *The blockchain cannot be described just as a revolution. It is a marching phenomenon, slowly advancing like a tsunami, and gradually enveloping everything along its way by the force of its progression.*” [1, s. 17]

Tampereella, 19.03.2019

Jarkko Nopanen

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

OP	Osuuspankki
POW	engl. Proof Of Work, todistus laskentakapasiteetin käytöstä
P2P	engl. Peer-to-Peer, vertaisverkko
QR-koodi	engl. Quick Response Code, nopean vasteen koodi
RFID	engl. Radio Frequency Identification, etätunnistus radioyhteyden välityksellä
SHA	engl. Secure Hash Algorithm, algoritmi tiedostojen tarkistusluvuille
URL	engl. Uniform Resource Locator, verkkosivun osoite

1. JOHDANTO

Lohkoketju on hajautettuja systeemejä hyödyntävä jaettu tietovarasto, johon tallennettu tieto säilyy eheänä ja muuttumattomana. Ensimmäisen kerran lohkoketjuteknologian julkaisi salanimellä Satoshi Nakamoto esiintyvä Bitcoinin perustaja vuonna 2008. Tämän jälkeen lohkoketjun sovelluskohteita on alettu tutkimaan myös laajasti muillakin aloilla ja lohkoketjuteknologiaan perustuen on muodostettu uusia sovelluksia.

Kohdeyritys on kiinnostunut lohkoketjun käytön tarjoamista uusista mahdollisuuksista. Tämän kandidaatintyön tutkimustavoitteena on selvittää, miten lohkoketjua voidaan hyödyntää osana kohdeyrityksen tuotantoketjua. Tavoitteen saavuttamiseksi tutkimus on jaettu kolmeen osaan.

Toisessa luvussa tutkitaan kirjallisuuslähteiden avulla aluksi lohkoketjuteknologian ominaisuuksia, luokittelua ja rakennetta. Lopussa tarkastellaan lohkoketjun käytöstä aiheutuvia hyötyjä ja haasteita sekä sovelluskohteita. Luvun tavoitteena on muodostaa yleiskäsitys lohkoketjuteknologiasta ja sen toimintaperiaatteista. Luvussa demonstroidaan myös lyhyesti tiivistefunktioiden toiminta.

Kolmas luku perustuu kohdeyrityksessä vierailuista ja haastatteluista saatuun informaatioon yrityksen tuotantoketjusta sekä yleistietoon toimitusketjuista. Luvun tavoitteena on määrittää kohdeyrityksen tuotantoketjun osat, niihin liittyvät toimijat ja tuotannon työvaiheet. Lisäksi käsitellään ketjussa esiintyviä ongelmakohtia. Nämä määritellään mahdollisimman tarkasti, mutta kandidaatintyön julkisen luettavuuden takia yrityssalaisuuksia suojellen.

Neljännessä luvussa on tarkoitus vastata kandidaatintyön tutkimustavoitteeseen, eli selvittää lohkoketjun hyödyntämismahdollisuuksia yrityksen tuotantoketjussa. Toiseen ja kolmanteen lukuun perustuen esitetään ehdotus lohkoketjun hyödyntämiselle yrityksessä. Luvussa selvitetään yritykselle parhaiten soveltuva lohkoketjuluokka, lohkoketjuun tallennettava data, ja tehdään ehdotuksesta havainnollistava malli. Luvussa tutkitaan myös lohkoketjun tuomat hyödyt ja jatkokehitysideat. Tämän lisäksi esitellään kappaleiden merkintätekniikoita, jotta fyysiset tuotteet on mahdollista saada identifioitua digitaaliseksi.

2. LOHKOKETJUTEKNOLOGIA

Tämän luvun alussa määritellään olennaisia lohkoketjun ominaisuuksia ja tarkastellaan lohkoketjujen luokittelua. Seuraavaksi tutkitaan lohkoketjun rakennetta, ja tiivistefunktioiden käyttöä osana lohkoketjua. Lopussa selvitetään lohkoketjun käytön hyötyjä ja haasteita sekä esitellään sovelluskohteita, joissa lohkoketjua nykyään käytetään.

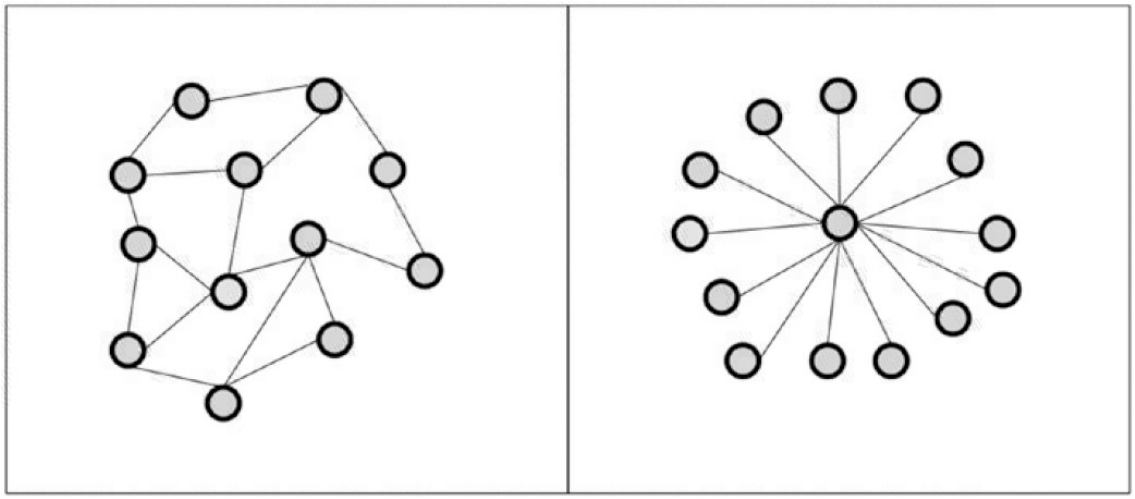
2.1 Lohkoketjun ominaisuudet

Seuraavissa alaluvuissa tarkastellaan lohkoketjun keskeisimpiä ominaisuuksia. Ensin selvitetään hajautetun systeemin toimintaperiaate, ja vertaillaan hajautetun ja keskitetyn systeemin eroja. Tämän jälkeen tarkastellaan hajautetun systeemin toteuttamista vertaisverkkojen (P2P, Peer-to-Peer) avulla. Lopuksi käsitellään lohkoketjun eheyttä ja muuttumattomuutta.

2.1.1 Hajautettu systeemi

Lohkoketju perustuu hajautettuihin systeemeihin. Hajautettu systeemi koostuu kahdesta tai useammasta solmukohdasta (engl. node), jotka toimivat yhdessä saavuttaakseen asetetun tavoitteen. Solmukohdat voivat lähettää ja vastaanottaa viestejä keskenään. Haasteena hajautetussa systeemissä on solmukohtien välinen koordinointi. Systeemin on toimittava, vaikka yhteys yksittäiseen solmukohtaan katkeaa tai solmukohta vioittuu. [2, s. 10] Lohkoketjun toiminnan ymmärtäminen on helpompaa, jos ensin perehtyy hajautettujen systeemien toimintaperiaatteeseen.

Kuvassa 1 on havainnollistettu hajautetun ja keskitetyn systeemin erot. Ympyrät esittävät systeemin komponentteja eli solmukohtia. Ympyröitä yhdistävät viivat ovat yhteyksiä komponenttien välillä. Hajautetussa systeemissä solmukohdat on yhdistetty toisiinsa epäsuorasti muiden solmukohtien kautta, joten niille ei ole olemassa yhteistä kontrolloivaa keskipistettä. Keskitetyssä systeemissä komponentit liittyvät yhteen keskuskomponenttiin, joka ohjaa systeemiä. [3, s. 10–11]



Kuva 1. *Hajautetun (vasen) ja keskitetyn (oikea) systeemin erot. [3, s. 11]*

Hajautetulla systeemillä saavutetaan parempi laskentateho verrattuna keskitettyyn systeemiin, jossa teho riippuu yksittäisen tietokoneen ominaisuuksista. Hajautetun systeemin laskentateho saadaan yhdistämällä kaikkien systeemissä olevien tietokoneiden resurssit, jolloin tehoa pystytään helposti kasvattamaan lisäämällä tietokoneita systeemiin. [3, s. 12]

Hajautetun systeemin alkukustannukset ovat suuremmat, mutta käyttö- ja huoltokustannukset ovat pienemmät verrattuna yhden supertietokoneen ylläpitokustannuksiin. Vaikka hajautetusta systeemistä hajoaa yksittäinen komponentti, systeemi kykenee jatkamaan toimintaansa normaalisti. [3, s. 12] Kuvasta 1 nähdään, että keskitetyn systeemin toiminta pysähtyy keskuskomponentin hajotessa, jolloin menetetään yhteys ympärillä oleviin solmukohtiin.

Koordinaation vaikeus on haasteena hajautetuille systeemeille, koska niissä ei ole keskeistä koordinaatiopistettä. Koordinointi toteutetaan verkon välityksellä. Kommunikointi verkossa vaatii ohjelmistolta kompleksisuutta, ja verkon kautta kommunikoidessa on myös turvallisuusongelmat otettava huomioon. [3, s. 22]

2.1.2 Vertaisverkko

Vertaisverkko (P2P-verkko) esitettiin ensimmäistä kertaa julkisuudessa vuonna 1999, kun amerikkalainen yliopisto-opiskelija Shawn Fanning perusti musiikinjakopalvelu Napsterin. Palvelun kautta käyttäjät etsivät musiikkitiedostoja, jotka sijaitsivat muiden käyttäjien kovalevyillä. Kun käyttäjä latasi tiedostoja, hän tarjoutui samalla jakamaan niitä muille käyttäjille. Napster kuitenkin suljettiin pian perustamisen jälkeen kopiosuojarikkomusten takia. [4]

Vertaisverkko voidaan määritellä täysin hajautetuksi itseorganisoituvaksi systeemiksi, joka käyttää jaettuja resursseja verkkoympäristössä. Vaikka vertaisverkko on alun perin

suunniteltu tiedostojen jakamispalveluihin, sen mekanismeja voidaan käyttää muidenkin jaettujen resurssien käsittelyyn, mikä tarjoaa uusia mahdollisuuksia Internetissä toimiville sovelluksille. [5, s. 9–10]

Hajautettu resurssien käyttö saadaan toteutettua P2P-verkon avulla. Vertaisverkossa jokainen tietokone voi toimia samanaikaisesti serverinä (engl. server) ja asiakkaana (engl. client) jakaen tiedostoja keskenään. Jokaisella käyttäjällä on samanlainen toiminnallisuus, mikä lisää järjestelmän joustavuutta. [5, s. 10–11] P2P-verkon solmukohdat yhdistyvät epäsuorasti toisiinsa ilman kolmatta osapuolta.

Perinteiset keskitetyt ratkaisut eivät enää riitä saavuttamaan kaikkia jatkuvasti laajenevan Internetin vaatimuksia. Keskitettyihin järjestelmiin on helppo hyökätä, ja niiden muokkaaminen on kallista ja vaikeaa. Vertaisverkot tarjoavat yksinkertaisempia ratkaisuja näihin ongelmiin. [5, s. 9–11] Vertaisverkko käyttää resursseja tehokkaammin kuin perinteinen verkko, ja vertaisverkko on myös vähemmän haavoittuvainen systeemissä esiintyville vioille [4].

2.1.3 Eheä ja muuttumaton tietovarasto

Edellisissä alaluvuissa esitetyissä täysin hajautetuissa systeemeissä on pystyttävä saavuttamaan tietojen eheys ja muuttumattomuus. Drescherin [3, s. 24–31] mukaan lohkoketjun ja vertaisverkkojen välinen yhteys voidaan määritellä hajautettujen systeemien eheyden avulla. Eheys tarkoittaa systeemin pysymistä turvallisena, yhteneväisenä ja virheettömänä. Eheyttä tarvitaan, jotta voidaan saavuttaa käyttäjien luottamus systeemiin. Lohkoketjun päätarkoituksena on eheyden saavuttaminen ja ylläpito täysin hajautetussa vertaisverkkojen avulla toteutetussa systeemissä. Eheyden saavuttaminen on helppoa, jos käyttäjien määrä ja luotettavuus ovat tiedossa, mutta haasteena on eheyden saavuttaminen tuntemattomien käyttäjien muodostamassa verkossa.

Muuttumattomuus on yksi lohkoketjun pääominaisuuksista. Tämä tarkoittaa, että lohkoketjuun lisättyjä tapahtumia on lähes mahdotonta poistaa tai muokata. [2, s. 23] Jos suurin osa prosessoritehosta on rehellisten solmukohtien hallinnassa, ne luovat pisimmän lohkoketjun ja syrjäyttävät hyökkääjät. Solmukohdat valitsevat aina pisimmän olemassa olevan lohkoketjun oikeaksi versioksi ja jatkavat sen kasvattamista. [6]

Hyökkääjien pitäisi saada 51 %:n hallinta kaikista solmukohdista muokatakseen lohkoketjuun tallennettuja tietoja [7]. Muuttumattomuuden ansiosta lohkoketjun avulla toteutettu hajautettu systeemi pysyy eheänä ja koskemattomana. Lohkoketjun muuttumattomuutta tarkastellaan vielä tarkemmin luvussa 2.3 lohkoketjun rakenteen muodostamisen yhteydessä.

2.2 Lohkoketjujen luokittelu

Lohkoketjut voidaan luokitella kolmeen eri kategoriaan sen perusteella, kenellä on oikeus nähdä ja muokata lohkoketjuun tallennettua tietoa. Kategoriat ovat julkinen, yksityinen ja näiden yhdistelmä eli hybridi.

Julkinen lohkoketju on tyypillisin kaikista lohkoketjuista. Se ei ole yksityisen tahon omistuksessa ja kuka vain voi liittyä siihen solmukohdaksi. Käyttäjillä on hallussaan paikallinen kopio lohkoketjusta ja solmukohdat valitsevat yksimielisesti lohkoketjusta käytettävän version. Käyttäjille voidaan myös maksaa palkkio lohkoketjun ylläpitämisestä. [2, s. 26] Julkisesta lohkoketjusta on esimerkkinä Bitcoin, johon perehdytään tarkemmin sovelluskohteiden yhteydessä luvussa 2.6.

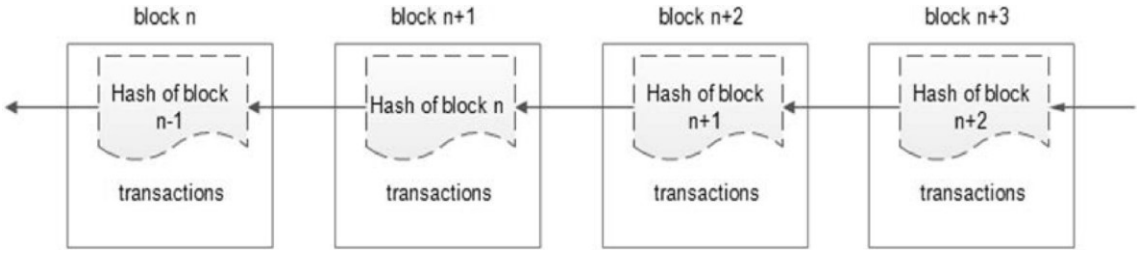
Yksityiset lohkoketjut ovat avoinna vain tietylle ennalta määrätylle ryhmälle, joka on päättänyt jakaa lohkoketjun keskenään [2, s. 26]. Yksityisen lohkoketjun avulla yritykset voivat luoda yhtymän, jossa yrityksen sisäiset transaktiot jaetaan osallistuvien käyttäjien saataville.

Yksityisen lohkoketjun vaarana on altistuminen keskitetyn systeemin riskeille. Keskitettyjä systeemejä turvallisempia yksityisistä lohkoketjuista tekee se, että hyökkääjän on hakkeroitava yli puolet solmukohdista muuttaakseen lohkoketjussa olevia transaktioita. Yleensä monissa solmukohdissa kuitenkin käytetään samanlaista teknologiaa, jolloin hyökkääjän on helppo hyödyntää haavoittuvuuksia toistuvasti. [8]

Hybridissä lohkoketjussa osa lohkoketjusta on yksityinen ja osa julkinen. Yksityistä osaa kontrolloi ennalta valittu ryhmä, ja julkinen osa on avoinna kaikille [2, s. 26]. Hybrideissä lohkoketjuissa on mahdollista saavuttaa lähes samantasoinen turvallisuus kuin julkisissa lohkoketjuissa. Kun yksityisessä osassa saavutetaan tietty määrä lohkoja, viimeisimmän lohkon tiiviste tallennetaan julkiseen osaan. Tällä tavalla hyökkääjän on lähes mahdotonta muuttaa lohkoketjun tietoja, kun lohko on tallennettu osaksi julkista lohkoketjua. [8] Hybridi lohkoketju toimii käytännöllisissä tarkoituksissa, joissa nopeus ja kustannustehokkuus ovat tärkeitä. Hybridi lohkoketju hyödyntää myös täysin lohkoketjun hajautusta ja muuttumattomuutta. [9]

2.3 Lohkoketjun rakenne

Lohkoketju on jaettu tietorakenne, joka voi sisältää monenlaista tietoa. Lohkoketjussa oleva tieto voi koostua esimerkiksi transaktioista (engl. transaction) [10, katso 16]. Transaktiot ovat aikajärjestyksessä ja ne on jaettu lohkoihin (engl. block) [2, s. 18]. Kuvassa 2 on havainnollistettu lohkoketjun muodostuminen yksittäisistä lohkoista.



Kuva 2. *Lohkoketjun muodostaminen [10]*

Lohkoketjun jokaiselle lohkolle on laskettu kryptografinen tiiviste (engl. hash), joka identifioi lohkon. Jokainen lohko sisältää transaktiodatan lisäksi edellisen lohkon tiivisteen. Kuvasta 2 huomataan kuinka kaikki lohkot kytkeytyvät toisiinsa tiivisteiden avulla. Lohkon *n* sisällä on tiiviste lohkosta *n-1*, lohko *n+1* sisältää lohkon *n* tiivisteen, ja sama periaate jatkuu lohkoketjun uusimpaan lohkoon (engl. head) asti. Tämä parantaa lohkoketjun turvallisuutta ja muuttumattomuutta. [10]

Jotta yksittäisessä lohkossa olevia tietoja voisi muokata, olisi muokattava myös kaikkia sitä seuraavia lohkoja. Ainoastaan ketjun aloittava lohko (engl. genesis block) ei sisällä edellisen lohkon tiivistettä. [2, s. 128] Drescherin [3, s. 71] mukaan yksi tärkeimmistä lohkoketjuun liittyvistä teknologioista on tiivisteiden laskenta tiivistefunktioilla (engl. hash function), joten niiden perustoiminta esitetään seuraavaksi.

Kryptografiset tiivistefunktiot ovat pieniä tietokoneohjelmia, jotka muuntavat mitä tahansa tietoa ennalta määrätyn pituisiksi numerosarjoiksi välittämättä alkuperäisen tiedon pituudesta. Tiivistefunktioita on erilaisia, riippuen niiden tuottaman numerosarjan pituudesta. Tiivistefunktiot luovat digitaalisen sormenjäljen mille tahansa datalle nopeasti ja deterministisesti. Deterministisyys tarkoittaa, että funktio tuottaa identtisen tiivisteen, jos sisääntulona on sama data kahdesti. Toisaalta funktion tiivisteet eivät myöskään voi olla identtisiä erilaisilla datasyötteillä. [3, s. 72]

Kryptografisen tiivistefunktion ulostulo on ennustamattomissa, vaikka syötettä vaihdettaisiin vain yhden kirjaimen verran. Lisäksi se on yksisuuntainen funktio, eli alkuperäistä dataa on mahdotonta palauttaa pelkän tiivisteen perusteella. [3, s. 73]

Tässä luvussa olevat kuvat ja taulukot on tehty Drescherin kirjan kuvien ja tietojen perusteella. Tiivisteiden laskemiseksi on käytetty yliopiston Linux-tietokoneen komentorivin kautta toimivaa OpenSSL-ohjelmaa. Tiivistefunktiona on käytetty SHA-256-funktiota (engl. Secure Hash Algorithm).

Muodostetaan taulukossa 1 olevasta datasta transaktioita, jotka lisätään lohkoketjuun. Sen jälkeen linkitetään lohkoketjun eri lohkot toisiinsa samaa tiivistefunktiota hyödyntäen. Muodostetaan 6 eri transaktiota kolmen omistajan (X, Y, Z) kesken. Taulukossa 1 on esitetty esimerkkidatojen nimet ja valittu omistajanvaihdokset.

Taulukko 1. *Siirrettävät datat ja omistajat.*

Data	**Vanha omistaja**	**Uusi omistaja**
data_1	X	Y
data_2	X	Z
data_3	Z	Y
data_4	Z	X
data_5	Y	X
data_6	Y	Z

Kuvassa 3 on laskettu tiivisteet taulukon 1 perusteella. OpenSSL-ohjelma laskee tiivisteen arvon halutulle transaktiolle komennolla:

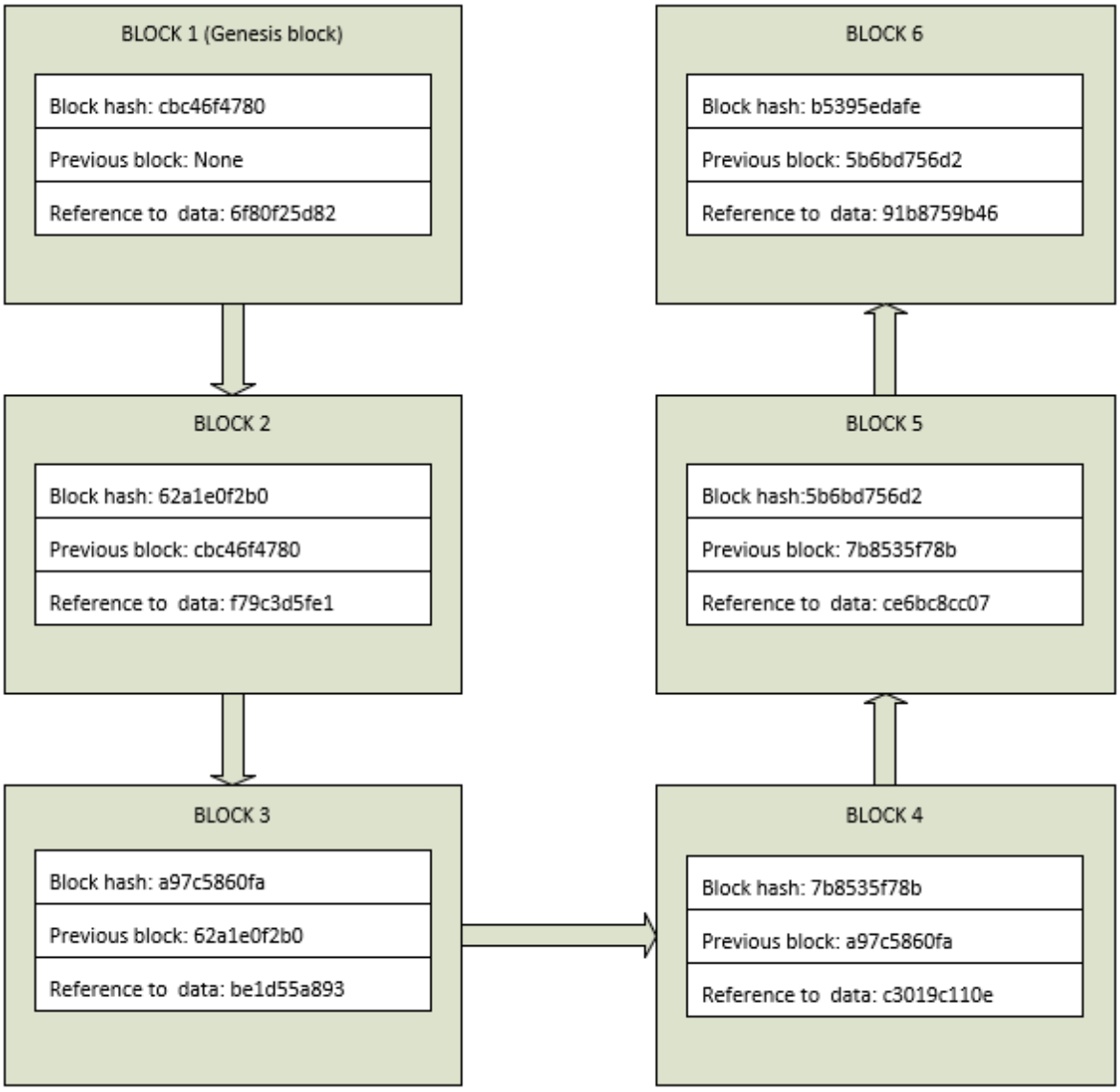
echo -n”*transaction_here*” | openssl dgst -sha256.

Saaduista tiivisteistä on mahdotonta päätellä alkuperäisiä funktiolle syötettyjä tietoja. Lohkojen tiivisteet on laskettu käyttäen vain kymmentä ensimmäistä merkkiä edellisestä tiivisteestä, jotta kuvat pysyvät selkeinä ja luettavina. Oikeasti lohkoketjun muodostamisessa käytettäisiin täysipituisia tiivisteitä. Tämän demonstraation tarkoituksena on havainnollistaa lohkoketjun rakentumista ja muuttumattomuutta mahdollisimman yksinkertaisesti.

```
bash-4.2$ echo -n "data_1 X Y" | openssl dgst -sha256
(stdin)= 6f80f25d827814beabadf9130233e73a8437ed933189ff751021746d29577a01
bash-4.2$
bash-4.2$ echo -n "data_2 X Z" | openssl dgst -sha256
(stdin)= f79c3d5fe1179ed375874c92abb01d6467d7b41de3bac41b9ac6a24c17acec11
bash-4.2$
bash-4.2$ echo -n "data_3 Z Y" | openssl dgst -sha256
(stdin)= be1d55a893a29f7573cef82d7cb53be6ddd63e59dd640337aac317411ef4fd08
bash-4.2$
bash-4.2$ echo -n "data_4 Z X" | openssl dgst -sha256
(stdin)= c3019c110ea47bec277383030061990e82c9d4e647b0c973cec29ea4ec5e111d
bash-4.2$
bash-4.2$ echo -n "data_5 Y X" | openssl dgst -sha256
(stdin)= ce6bc8cc07d2dade63e9f21f8e70963a36e59cfe0888de1032d3912a395a620a
bash-4.2$
bash-4.2$ echo -n "data_6 Y Z" | openssl dgst -sha256
(stdin)= 91b8759b460205c9d8d82ef70430aa15ea5ee1bac4babb07d671155079a4b926
bash-4.2$
bash-4.2$ echo -n "None 6f80f25d82" | openssl dgst -sha256
(stdin)= cbc46f4780d8053ae07f6100a1a60dc712f723dcf26179cbe6ce148828b3c0cb
bash-4.2$
bash-4.2$ echo -n "cbc46f4780 f79c3d5fe1" | openssl dgst -sha256
(stdin)= 62a1e0f2b025e6da9315a887e2b7f864ca909a02c3360e71374c2f865dc495cb
bash-4.2$
bash-4.2$ echo -n "62a1e0f2b0 be1d55a893" | openssl dgst -sha256
(stdin)= a97c5860fa193adf713a7d105b0a59d6ab5800ce786c93bb60d82eede5640f81
bash-4.2$
bash-4.2$ echo -n "a97c5860fa c3019c110e" | openssl dgst -sha256
(stdin)= 7b8535f78b926394070202292dd3f1d108dea8c889ec1011f41f254c0c58d36b
bash-4.2$
bash-4.2$ echo -n "7b8535f78b ce6bc8cc07" | openssl dgst -sha256
(stdin)= 5b6cd756d2101c9c79d8830452e9cc79a3e01f6899f6e8da28e57fd43e3118d8
bash-4.2$
bash-4.2$ echo -n "5b6bd756d2 91b8759b46" | openssl dgst -sha256
(stdin)= b5395edafee2532d186d39d2d3f72875a8557f08de3255745cf9be0aa16f265d
bash-4.2$
```

Kuva 3. *Tiivisteiden laskenta kuudelle eri transaktiolle.*

Kuvassa 4 jokaisen transaktion tiiviste on sisällytetty omaan lohkoonsa demonstroiden lohkoketjun muodostamista. Edellisen lohkon tiivisteestä (engl. previous block) ja lohkon transaktion tiivisteestä (engl. reference to data) on laskettu kyseiselle lohkolle tiiviste (engl. block hash). Ensimmäisellä lohkolla ei ole edeltäjää, joten sen tiiviste on laskettu edellisen lohkon arvolla *None.*



Kuva 4. *Esimerkkitransaktioista muodostettu lohkoketju.*

Tiivisteiden laskennassa käytetään lisäksi vaikeustasoa (engl. nonce), jolla määritellään lohkojen syntymisen aikaväli. Lohkoihin sisältyy myös aikaleima (engl. timestamp), joka on jätetty kuvasta pois selkeyden takia. Tärkeää on havaita, kuinka jokainen lohko osoittaa edelliseen lohkoon linkittäen ketjun oikeaan järjestykseen. Lohkojen määrän kasvaessa tietojen väärentäminen ei ole käytännössä mahdollista, koska laskentatehoa tarvittaisiin saavuttamaton määrä.

2.4 Lohkoketjun käytön hyötyjä

Läpinäkyvyys on yksi lohkoketjun suurimmista hyödyistä kaikenkokoisille yrityksille. Lohkoketjuteknologia mahdollistaa monien prosessien ja transaktiopalveluiden tekemisen läpinäkyvämmäksi ilman kolmannen osapuolen osallistumista. Muutokset julkiseen lohkoketjuun ovat kaikkien osapuolten nähtävillä. [7]

Yritykset voivat parantaa toimitusketjun hallintaa materiaalien tarkemman ja läpinäkyvämmän jäljityksen avulla. Lohkoketjun avulla on mahdollista digitalisoida fyysiset tuotteet, ja luoda muuttumaton tietovarasto kaikista tapahtuneista transaktioista. Tuotteen historian parempi läpinäkyvyys tarjoaa näkyvyyttä yrityksen lisäksi myös muille toimitusketjun osapuolille. [11]

Koska teknologian avulla tieto tallennetaan hajautetusti, systeemillä ei ole yhtä kontrolloivaa keskipistettä. Tieto säilyy niin kauan, kuin yksikin solmukohta on toiminnassa. Keskitetyssä systeemissä serverillä olevien tietojen häviäminen aiheuttaisi systeemin toiminnan keskeytymisen. Koska kaikki tapahtumat lisätään vain yhteen tietovarastoon, myös ongelmat useiden tietovarastojen synkronointiin liittyen voidaan eliminoida. [12]

2.5 Lohkoketjun käytön haasteita

Vaikka lohkoketjuteknologialla on monia ilmeisiä hyötyjä, niiden saavuttaminen vaatii uuden teknologian käyttöönoton, ja vanhojen keskitettyjen järjestelmien muuntamisen hajautetuksi. Vaihdon suorittaminen saattaa olla haastavaa, ja vaatii tarkkojen strategioiden ja suunnitelmien tekemistä ennen toteutusta. [11] [12] Koska lohkoketjun käyttöönotto vaatii merkittävän siirtymän hajautettuun verkkoon, käyttäjille ja operaattoreille on tiedotettava asiasta hyvissä ajoin. [11]

Lohkoketjuteknologian käyttöönotto vaatii suuria muutoksia olemassa oleviin systeemeihin. Yritysten on otettava tämä huomioon, sillä alkuinvestoinnit voivat olla merkittäviä, ja saattavat rajoittaa yritysten lohkoketjun käytön aloittamista. Lohkoketjuteknologian kehitys on vielä kesken ja teknologia on uutta, joten siirtonopeuksissa ja varmennuksissa on ollut ongelmia. Nämä ongelmat pitää huomioida, jotta teknologiaa pystytään hyödyntämään täydellä potentiaalilla. [12]

Tiedon virtaamisen saavuttamiseksi kaikki toimitusketjun vaiheet ja tuotteet pitää saada digitaaliseksi. Tämä vaatii tuotteiden ja osien merkitsemistä. Tuotteiden merkitsemisen voi liittää olemassa olevaan toimitusketjuun hyvissä ajoin lohkoketjun toteutuksen valmisteluissa. [11] Eri merkitsemistapoja vertaillaan neljännessä luvussa ja valitaan niistä yritykselle sopivin.

Seuraavassa luvussa tarkastellaan lohkoketjun sovelluskohteita, joista ensimmäinen on virtuaalivaluutta Bitcoin. Bitcoinin transaktioita varmennettaessa kaikki solmukohdat

käyttävät suuren määrän energiaa, josta suurin osa menee hukkaan [12]. Pienemmissä lohkoketjuissa tätä ongelmaa ei kuitenkaan esiinny, koska solmukohtien määrä on hyvin vähäinen verrattuna julkisen lohkoketjun käyttäjämäärään.

2.6 Lohkoketjun sovelluskohteita

Lohkoketju on alun perin kehitetty Bitcoinille, joka on virtuaalinen kryptovaluutta. Tämän takia lohkoketju-käsite yhdistetään yleensä virtuaalivaluuttoihin. Lohkoketjulla on kuitenkin paljon muitakin sovelluskohteita. [3, s. 35–36] Tässä luvussa esitellään Bitcoinin lisäksi lohkoketjun käyttöä komposiittimateriaalien toimitusketjuissa, ja kerrotaan lyhyesti muista sovelluskohteista.

2.6.1 Virtuaalivaluutta Bitcoin

Nakamoton [6] mukaan kolmannen osapuolen pois jättäminen elektronisen rahan siirrossa vaatii kaksoiskuluttamisen (engl. double-spending) estämistä uuden teknologian avulla. Systeemi perustuu luottamuksen sijaan kryptografiseen todisteeseen. Bitcoinissa ketkä vain kaksi tahoa voivat siirtää rahaa toisilleen suoraan ilman kolmatta osapuolta. Vertaisverkon avulla transaktioille luodaan aikaleimat, ja tiivistetään ne yhteneväksi ketjuksi. Ketjun muodostamisessa käytetään algoritmia (engl. Proof-of-Work, POW), jonka laskemiseen tarvitaan suuri määrä laskentatehoa. Algoritmin uudelleenlaskeminen kaikille lohkoille vaaditaan, jotta ketjussa olevia tietoja pystyisi muokkaamaan.

Verkon ylläpito perustuu seuraaviin vaiheisiin. Ensimmäisessä vaiheessa uudet transaktiot tulevat näkyville kaikille solmukohdille. Sen jälkeen jokainen solmukohta kerää transaktiot uuden lohkon sisälle. Solmukohdat kilpailevat siitä, kuka ratkaisee algoritmin ensimmäisenä kyseiselle lohkolle. Kun POW on ratkaistu, lohko julkaistaan kaikille muille solmukohdille. Jos lohkossa olevat transaktiot ovat käyttämättömiä ja POW on ratkaistu oikein, lohko lisätään lohkoketjun päähän, ja solmukohdat alkavat ratkaisemaan uutta lohkoa. Lohkon ensimmäinen ratkaisija palkitaan uudella Bitcoinilla, mikä kannustaa solmukohtia tukemaan verkkoa. Jos lohkoketjusta julkaistaan useita versioita, vain pisin niistä säilyy oikeana, ja muut versiot hylätään. [6]

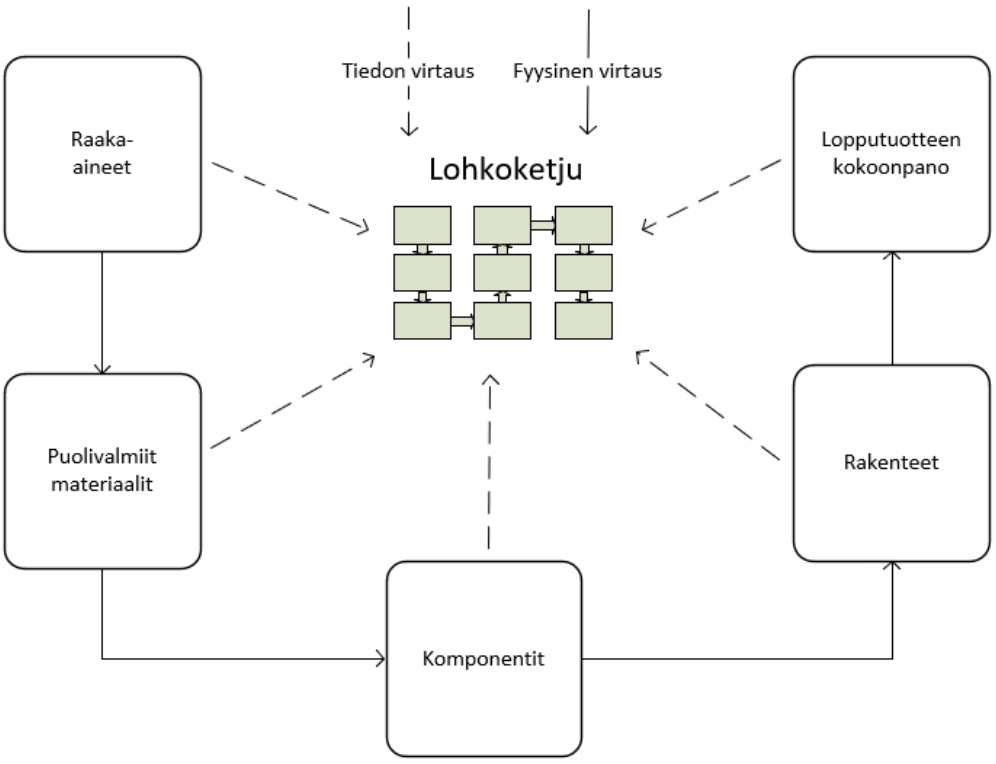
2.6.2 Komposiittimateriaalien toimitusketjut

Toimitusketjut yhdistävät tuotteiden valmistusprosessiin osallistuvat tekijät. Toimitusketju sisältää sopimusten käsittelyä, maksuja, pakkaamista ja kuljetuksia. Systeemin kompleksisuus johtaa korkeisiin siirtokuluihin. Virheitä tapahtuu myös helpommin, jos paperityöt tehdään manuaalisesti. Lisäksi monimutkaiset systeemit saattavat sisältää turvattomia työskentelyolosuhteita tai laittomia tuotantoprosesseja. [13]

Lohkoketjun avulla voidaan jäljittää tuotteita, jotka kulkevat toimitusketjun läpi. Tuotteet identifioidaan esimerkiksi viivakoodeilla tai QR-koodeilla. Tuotteiden siirtyessä toimitusketjussa eteenpäin, käyttäjät tallentavat siirron lohkoketjuun. Samalla lohkoketjuun tallentuu aikaleima siirrosta. [13]

Lentokoneteollisuudessa valmistetaan komposiittimateriaaleja, joita käytetään lentokoneiden osien tuotannossa. Lentokoneiden valmistuksessa olevat tiukat standardit vaativat käytettyjen materiaalien jäljitettävyyttä. Lohkoketjuteknologian avulla voidaan taata muuttumattomat historiatiedot materiaalien tuotantoon, kuljetukseen, käsittelyyn ja varastointiin. [14] Lohkoketjun avulla saavutetaan siis toimitusketjulle standardien mukaiset jäljitystiedot alusta loppuun asti.

Lohkoketjun hyödyntäminen komposiittimateriaalien tuotantoketjussa on havainnollistettu kuvassa 5. Tuotantoketju alkaa raaka-aineista, joista tehdään puolivalmiita materiaaleja. Komponentteihin kuuluu esimerkiksi hiilikuidusta valmistettu moottoritunneli. Komponenteista muodostetaan rakenteita, jotka siirtyvät lopullisen tuotteen kokoonpanovaiheeseen. [14] Eri vaiheet muodostavat systeemin solmukohdat, joiden väliset transaktiot tallennetaan lohkoketjuun.



Kuva 5. *Lohkoketjun hyödyntäminen komposiittimateriaalien tuotantoketjussa, muokattu lähteestä. [14]*

Transaktioihin voidaan liittää tietoa esimerkiksi hinnasta, päivämäärästä, laadusta ja tuotteen tilasta. Lisäksi lohkoketjun avulla voidaan tallentaa tuotteiden tarkempia ominaisuuksia kuten leveys, paksuus ja muoto. Porausten, hitsauksen, pintakäsittelyn ja kokoonpanon aikaisia tietoja voidaan myös lisätä lohkoketjun transaktioihin. [14]

Lohkoketjulla on jäljitettävyyden ja ominaisuuksien tallentamisen lisäksi mahdollista ohjata tuotantosertifikaatteja, jotka on yhdistetty komponenttien laatuun ja alkuperään. Jälkeenpäin tietoja voidaan tarkastella laatuongelmien yhteydessä tuotteen elinkaaren myöhemmässä vaiheessa, mikä on erittäin tärkeää viallisten tuotteiden takaisinlähetyksissä. Tietojen luotettavuus on parempi verrattuna perinteisiin menetelmiin, koska tietojen syöttäminen lohkoketjuun on varmennettu. [14]

2.6.3 Muita sovelluskohteita

Uutena sovelluskohteena Suomessa on vuonna 2019 käyttöönotettu pilottihanke asuntokaupan sähköistämisestä lohkoketjuteknologian avulla. Järjestelmä perustuu Corda-lohkoketjualustaan, joka on suljettu lohkoketjuympäristö. Osapuolina lohkoketjussa on ennalta tarkistettuja pankkeja kuten Aktia, Danske Bank, OP ja S-Pankki. Hyötynä on aluksi paperien käsittelystä eroon pääseminen, ja kauppojen tekeminen täysin digitaalisesti. [15] [16]

Edellisten sovelluskohteiden lisäksi lohkoketjua voidaan käyttää muun muassa 3D-tulostuksessa mallitiedostojen jakamiseen [13]. Lohkoketjua on hyödynnetty myös timanttien toimitusketjuissa jäljittämään luotettavasti tuotteiden alkuperä sekä tunnistamaan väärennökset [7] [17].

3. KOHDEYRITYKSEN TOIMITUS- JA TUOTANTOKETJU

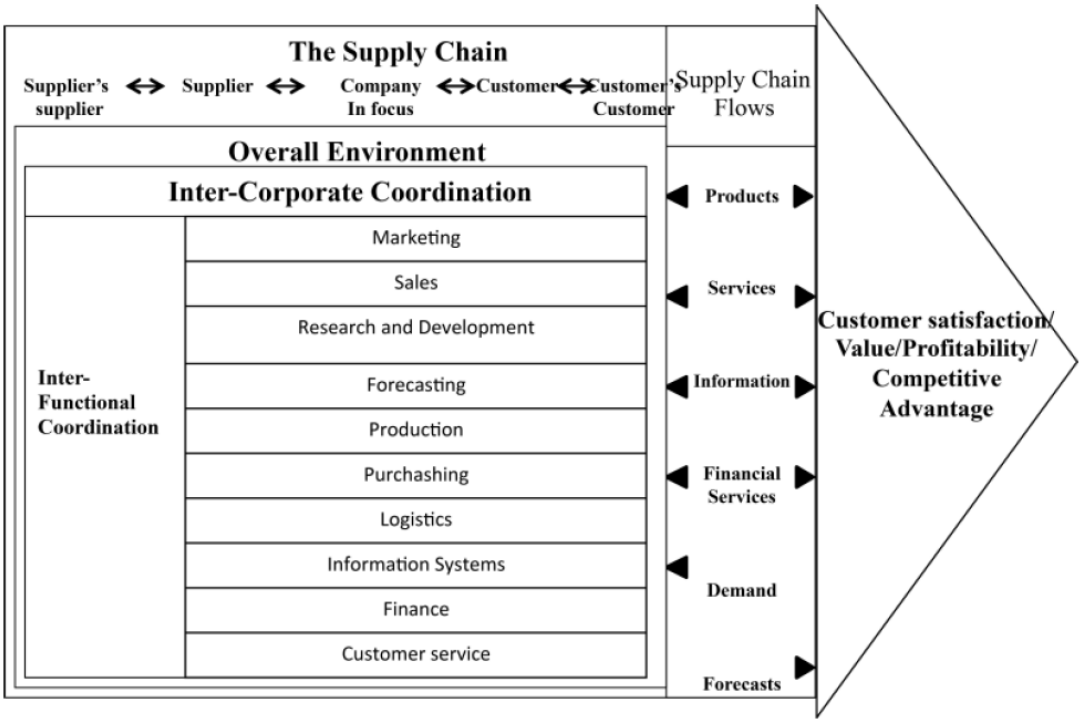
Koska opinnäytetyöt ovat julkisesti luettavissa, tässä luvussa käsitellään vain yleisesti toimitusketjujen rakennetta yrityssalaisuuksien säilyttämiseksi. Toimitusketjun perusperiaate on samanlainen lähes kaikissa fyysisiä tuotteita valmistavissa yrityksissä, joten lohkoketjun hyödyntämisen kannalta tarkat yksityiskohdat eivät ole oleellisia. Lisäksi luvussa tarkastellaan kohdeyrityksessä valmistettavan tuotteen tuotantoketjussa olevia työvaiheita, ja ketjun aikana havaittuja ongelmakohtia, joihin voidaan löytää parannusehdotuksia lohkoketjun avulla.

3.1 Toimitusketju yleisesti

Toimitusketju (engl. supply chain) tarkoittaa kaikkia tuotteen elinkaareen liittyviä toimintoja raaka-aineesta asiakkaalle. Toimitusketjuun sisältyy materiaalivirtojen lisäksi tietovirrat. Materiaali ja tieto kulkevat molempiin suuntiin toimitusketjua. [18, s. 5–7]

Toimitusketjujen hallinta (engl. supply chain management) voidaan määritellä liiketoiminnan systemaattiseksi ja strategiseksi koordinaatioksi tietyssä yrityksessä. Toimitusketjujen hallinnan tarkoituksena on parantaa yrityksen toimitusketjun suorituskykyä, ja saavuttaa kilpailukykyistä etua pitkällä aikavälillä. [18, s. 5–7]

Kuvassa 6 on yleismalli toimitusketjusta, johon sisältyy kaikki osallistujat raaka-aineiden toimittajasta loppukäyttäjään asti. Keskellä toimitusketjua on esitetty tarkasteltavana oleva yritys (engl. company in focus). Nuolet osoittavat materiaali- ja tietovirtausten suunnat.



Kuva 6. *Toimitusketjun yleismalli [19]*

Yrityksen sisäiseen koordinointiin kuuluu markkinointi, myynti, tuotekehitys, ennusteet, tuotanto, osto, logistiikka, tietojärjestelmät, talous ja asiakaspalvelut. Kysyntä tulee asiakkaalta yrityksen suuntaan, ja ennusteet tehdään kysynnän perusteella asiakkaan suuntaan. Yhdessä näiden kaikkien tarkoituksena on parantaa asiakastyytyväisyyttä ja tuottavuutta ja näin saavuttaa kilpailuetua. Toimitusketju on siis toistensa kanssa vuorovaikutuksessa olevista alisysteemeistä muodostuva kokonaisuus [18, s. 5–7].

3.2 Toimitusketjun osapuolien oikeudet dataan

Tärkeänä osana kohdeyrityksen toimitusketjun hahmottamista tehdessä on rajata eritasoisia oikeuksia ketjussa liikkuvaan dataan, jotta neljännessä luvussa voidaan valita käytettäväksi julkinen, yksityinen tai hybridi lohkoketju. Oikeudet on määritelty Savinaisen haastattelun [Liite A] pohjalta.

Toimittajien ei tarvitse tietää kaikkea yrityksen sisäistä tietoa, ja näin ollen toimittajien oikeuksia on rajoitettu. Toimihenkilöihin kuuluu markkinointi, myynti, osto ja tuotekehitys. Tämän ryhmän on tarkoitus päästä käsiksi kaikkeen ketjussa olevaan dataan. Tehtaan tuotannossa työskenteleviltä työntekijöiltä on rajoitettava vain kustannustiedot, mutta muu ketjussa oleva data saa olla näkyvillä. Asiakkaiden oikeudet rajataan hyvin suppeaksi, jotta he pääsevät käsiksi vain välttämättömimpään tietoon. Taulukossa 2 on määritelty oikeudet eri väreillä eroteltuna. Värien merkitys on selitetty taulukon oikealla puolella.

Taulukko 2. *Osapuolien oikeuksien määrittely.*

	Toimittajat	Toimihenkilöt	Työntekijät	Asiakkaat
Jäljitystiedot				
Kustannustiedot				
Tuotantotiedot				
Tuotetiedot				
Mittaustiedot				
Laatusertifikaatit				
Läpimenoaika				

Täydet oikeudet
Rajoitetut oikeudet
Suppeat/ei oikeuksia

Tärkeää taulukosta on huomata, että oikeudet on pidettävä erittäin rajallisina tietyille ryhmille, kun taas toiset ryhmät saavat täydet oikeudet ketjussa liikkuviin tietoihin. Tämän huomion pohjalta pystytään myöhemmin valitsemaan parhaiten soveltuva lohkoketjuluokka.

3.3 Tuotantoketjun työvaiheiden määrittely

Kohdeyrityksen tuotantoketjuun kuuluu monia erilaisia työvaiheita, joista esimerkkejä on valittu taulukkoon 3. Lisäksi työvaiheille on valikoitu tyypillisiä tietoja, joita lohkoketjuun on mahdollista tallentaa. Työvaiheet on määritelty yrityksessä vierailun perusteella.

Taulukko 3. *Tuotantoketjun työvaiheet ja niistä kerättävät tiedot.*

Työvaihe	Kerättävät tiedot
Raaka-aihio toimittajalta	Pvm, toimituserä, toimittaja
Sorvaus	Pvm, käytetyt työkalut
Lämpökäsittely	Pvm, kesto, lämpötila
Hionta	Pvm, työntekijä, kesto
Mittaus	Pvm, ulkomitat, sisämitat, poikkeama sallitusta, mittaaja, hylätty/hyväksytty
Kokoonpano	Pvm, työntekijä, kerätyt osat, osapuutteet, ongelmat, momentit
Testaus	Pvm, työntekijä, vuoto, testauksen pituus, testipenkin numero, hylätty/hyväksytty
Pesu	Pvm, työntekijä
Maalaus	Pvm, työntekjä, väri
Pakkaus	Pvm, työntekijä
Toimitus	Pvm, työntekijä, kohde

Tyypillisessä tuotteen toimitusketjussa ensin toimittajalta saadaan raaka-aihio, josta työstetään eri työvaiheiden avulla valmis kappale. Mittausvaiheessa varmistetaan, että kappale on sallittujen rajamittojen sisäpuolella. Kokoonpanovaihe sisältää monien kappaleiden yhteensovittamisen, jonka jälkeen tuote testataan testipenkissä. Testin mennessä läpi tuote pestään, maalataan ja pakataan toimitusvalmiiksi.

Eri vaiheissa kerättäviä tietoja voisivat olla taulukon mukaisesti päivämäärä, toimituserä, käytetyt työkalut, käsittelyjen parametrit, mittaustiedot, työn suorittaja, kerätyt osat

sekä puutteet ja ongelmat. Nykyisessä järjestelmässä esimerkiksi mittaustulokset tallennetaan vain paikallisesti, ja etsittäessä tietylle tuotteelle suoritettujen työvaiheiden tietoja, aikaa menee turhaan niiden jäljittämiseen eri tietokannoista [Liite A].

3.4 Ongelmakohdat tuotantoketjussa

Suurimpana ongelmana tuotantoketjussa on läpinäkyvyyden puuttuminen tuotteiden työvaiheiden välillä. Joskus kappaleilla on monen päivän jaksoja, jolloin ei pystytä määrittämään kappaleen liikkeitä tarkasti. [Liite A] Koska tietoja myös tallennetaan moneen toisistaan irralliseen paikkaan, tietojen löytäminen jälkikäteen on haastavaa. Tietoja saattaa olla pilvipalveluissa, käyttäjien paikallisilla kovalevyillä ja papereille tallennettuina.

Toinen ratkaistava ongelma lohkoketjun käytön kannalta on kappaleiden merkinnän puutteellisuus [Liite A]. Jotta kappale voidaan tallentaa osaksi lohkoketjua, kappale on pystyttävä identifioimaan luotettavasti ja pysyvästi. Tähän ongelmaan esitetään ratkaisu neljännen kappaleen alussa, jotta voidaan tehdä havainnollistava malli lohkoketjun hyödyntämisestä.

4. TUOTANTOKETJUN LÄPINÄKYVYYDEN PARANTAMINEN LOHKOKETJUN AVULLA

Lohkoketjun hyödyntäminen vaatii tuotantoketjussa käsiteltävien kappaleiden luotettavan ja pysyvän merkinnän, jotta kappaleet saadaan identifioitua digitaaliseen muotoon lohkoketjun käyttöä varten. Tämän luvun alussa vertaillaan kappaleiden merkintätapoja, ja valitaan niistä yritykselle sopivin. Merkintätavan valinnan jälkeen valitaan yritykselle sopivin lohkoketjuluokka, jonka jälkeen esitetään havainnollistava malli lohkoketjun käyttämisestä. Lopuksi tarkastellaan tämän tutkimuksen ulkopuolelle jääviä jatkokehityskohteita.

4.1 Kappaleiden merkintätekniikat

Vertailtaviksi on valittu kolme eri tekniikkaa, jotka ovat viivakoodi, QR-koodi (engl. Quick Response code) ja RFID (engl. Radio Frequency Identification). Tässä luvussa esitellään ensin tekniikoiden ominaisuuksia. Sen jälkeen suoritetaan vertailu eri tekniikoiden välillä, ja valitaan niistä yritykselle sopivin luotettavuuden ja käytettävyyden kannalta.

4.1.1 Viivakoodi

Viivakoodi on sarja pystysuoria erilevyisiä palkkeja. Viivakoodia käytetään tiedon syöttämiseen tietokonejärjestelmään [20]. Koodiin voidaan sisällyttää numeroita ja kirjaimia [21]. Useimmat viivakoodit ovat itsetarkastavia, eli virheiden mahdollisuus on pieni.

Viivakoodeja luetaan optisella skannerilla, joka on yhdistetty tietokoneeseen. Skanneri voi olla kädessä pidettävä tai kiinnitetty pysyvästi alustaan, jonka edestä kappaleet kulkevat. Viivakoodeja käytetään esimerkiksi prosessoiduissa ruoissa, lääkkeissä, auton osissa ja kirjaston kirjoissa. Viivakoodin käytön hyötynä on yksityiskohtaisen tiedon käsittely viivakoodin lukuhetkellä, mutta fyysinen koko rajoittaa käyttöä joissain tapauksissa. [22]

4.1.2 QR-koodi

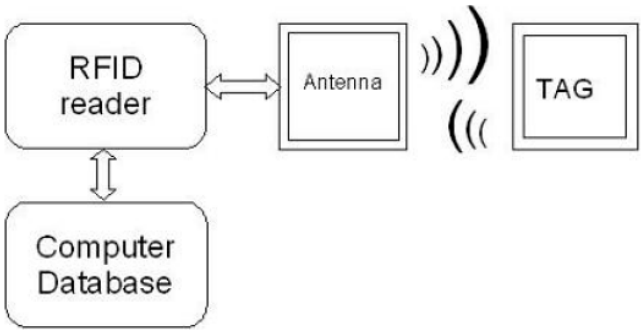
QR-koodi on viivakoodityyppi, joka koostuu neliönmuotoisista mustista ja valkoisista kuvioista, jotka koodaavat dataa sisälleen. Mustat ja valkoiset neliöt esittävät numeroita 1–9, kirjaimia A–Z tai erikoismerkkejä. Kulmissa olevat neliöt mahdollistavat koodin suuntaamisen oikein päin ohjelman sisällä. [23]

Suurin mahdollinen koodi (versio 40) on 177x177-pikselin kokoinen matriisi. Tähän koodiin mahtuu 7089 numeroa tai 4296 kirjainmerkkiä. QR-koodia käytetään yleensä mainonnassa esittämään web-sivun URL-osoitetta. Lisäksi yksi käyttökohde on erilaisten tapahtumien pääsylipuissa. Kuvioita voidaan lukea tietokoneeseen liitetyllä skannerilla tai älypuhelimen kameralla. [23] QR-koodit ovat pienempikokoisia kuin viivakoodit ja niiden tietokapasiteetti on suurempi [21].

4.1.3 RFID

RFID (engl. Radio Frequency Identification) on teknologia, jolla voidaan identifioida tiettyjä kohteita, ja lukea ja kirjoittaa tietoa radiosignaalien avulla. Lukemiseen ei tarvita optista yhteyttä kohteen ja lukujärjestelmän välille. [24]

RFID-järjestelmä koostuu RFID-tagista, lukijasta ja tietovarastosta. Lukijassa oleva antenni keskustelee saattomuistin (engl. tag) kanssa keräten sisällä olevat tiedot. Lukija voi olla liikuteltava kädessä pidettävä versio tai kiinteästi asennettava laite. Saattomuisti on pieni osa, joka koostuu antennista, mikrosirusta ja kotelosta. Koteloita on eri materiaaleja ja kokoja. [21] [24] Kuvassa 7 on havainnollistettu komponentit ja niiden toiminta.



Kuva 7. *RFID-tekniikan komponentit [24]*

Saattomuistin sisällä olevassa mikrosirussa on muistia muutamasta kymmenestä tavusta 32:een kilotavuun. Saattomuistit voidaan asettaa vain-luku muotoon tai vaihtoehtoisesti luku- ja kirjoitusmuotoon. Saattomuisteja on passiivisia sekä aktiivisia, joista aktiivisissa on lisäksi sisäinen virtalähde, ja ne ovat kalliimpia. [24]

4.1.4 Merkintätekniikan valinta

Taulukossa 4 on esitetty eri tekniikoiden ominaisuudet ja vertailtu soveltuvuutta kohdeyrityksen tuotantoketjuun. Ominaisuudet on luokiteltu edellisten alalukujen teoriatutkimuksen pohjalta. Vertailun tulokset on tarvittaessa esitetty suhteessa toisiinsa, eli esimerkiksi fyysiseltä kooltaan pieni on tässä tapauksessa muihin kahteen verrattuna pienin.

Taulukko 4. *Merkintätekniikoiden vertailu*

	Viivakoodi	**QR-koodi**	**RFID**
Tallennuskoko	Riippuu pituudesta	7089 numeroa tai 4296 kirjainmerkkiä	10b-32kb
Tiedon tyyppi	Numerot ja kirjaimet	Numerot ja kirjainmerkit	Ei standardoitua formaattia
Fyysinen koko	Keskisuuri	Pieni	Suuri
Pariston tarve	Ei	Ei	Kyllä/ei
Tiedon muokkaus	Ei	Kyllä/ei	Kyllä/ei
Kestävyys	Kestävä	Kestävä	Heikko
Käytön helppous	Melko helppo	Melko helppo	Helppo
Hinta	Halpa	Halpa	Kallis
Luotettavuus	Hyvä	Hyvä	Heikko (saattaa irrota)

RFID-teknologia voisi olla toimiva, jos tietoa tarvitsisi tallentaa paljon. Kuitenkin ideana on käyttää merkintää vain kappaleen identifioimiseen, joten RFID-teknologia ei ole tarpeellinen. Tietoa ei ole myöskään tarkoitus muokata tallentamisen jälkeen, vaan se halutaan saada kappaleeseen pysyvästi. Myös RFID-komponenttien hajoaminen kovassa käytössä on riskitekijä.

Viivakooditeknologia olisi yksinkertaisuutensa puolesta sopiva vaihtoehto, ja tallennuskoko riittäisi sarjanumeron tallentamiseen. Fyysisen kokonsa puolesta viivakoodin käytössä saattaa kuitenkin tulla ongelmia kappaleiden ollessa pienikokoisia. QR-koodi puolestaan on pienempi kuin viivakoodi, ja QR-koodiin voidaan tallentaa sarjanumero yhtä helposti kuin viivakoodiin. QR-koodiin on mahdollista tallentaa tarvittaessa esimerkiksi myös osan nimeävä tunniste.

Merkintätekniikaksi valitaan edellisen vertailun perusteella QR-koodi pienen kokonsa ansiosta verrattuna normaaliin viivakoodiin. RFID jätetään pois luotettavuuden puutteen ja kalliimman teknologian takia.

4.2 Kohdeyritykseen soveltuva lohkoketjuluokka

Kolmannessa luvussa tarkasteltiin toimitusketjussa olevien osapuolien oikeuksia lohkoketjuun tallennettaviin tietoihin. Tarkastelun perusteella havaittiin, että oikeudet tulee pystyä asettamaan hyvin rajallisiksi asiakkaille, kun taas toimihenkilöiden on päästävä tarkastelemaan kaikkea ketjuun tallennettavaa dataa. Työntekijöille on pystyttävä antamaan oikeudet suurimpaan osaan tiedoista, mutta jättämään kustannustiedot pois näkyviltä.

Julkinen lohkoketju ei sovellu yrityksen tarkoituksiin, koska siinä tiedot ovat julkisesti saatavilla kaikille halukkaille. Tämän takia yrityssalaisuudet menettäisivät merkityksensä. Julkisen lohkoketjun ongelmana on myös runsas energiankäyttö ja hitaus [9].

Yksityinen lohkoketju puolestaan sulkee pois asiakkaiden mahdollisuudet tarkastella heille kohdennettuja tietoja. Jos lohkoketjusta tehdään täysin yksityinen tietyn ennalta

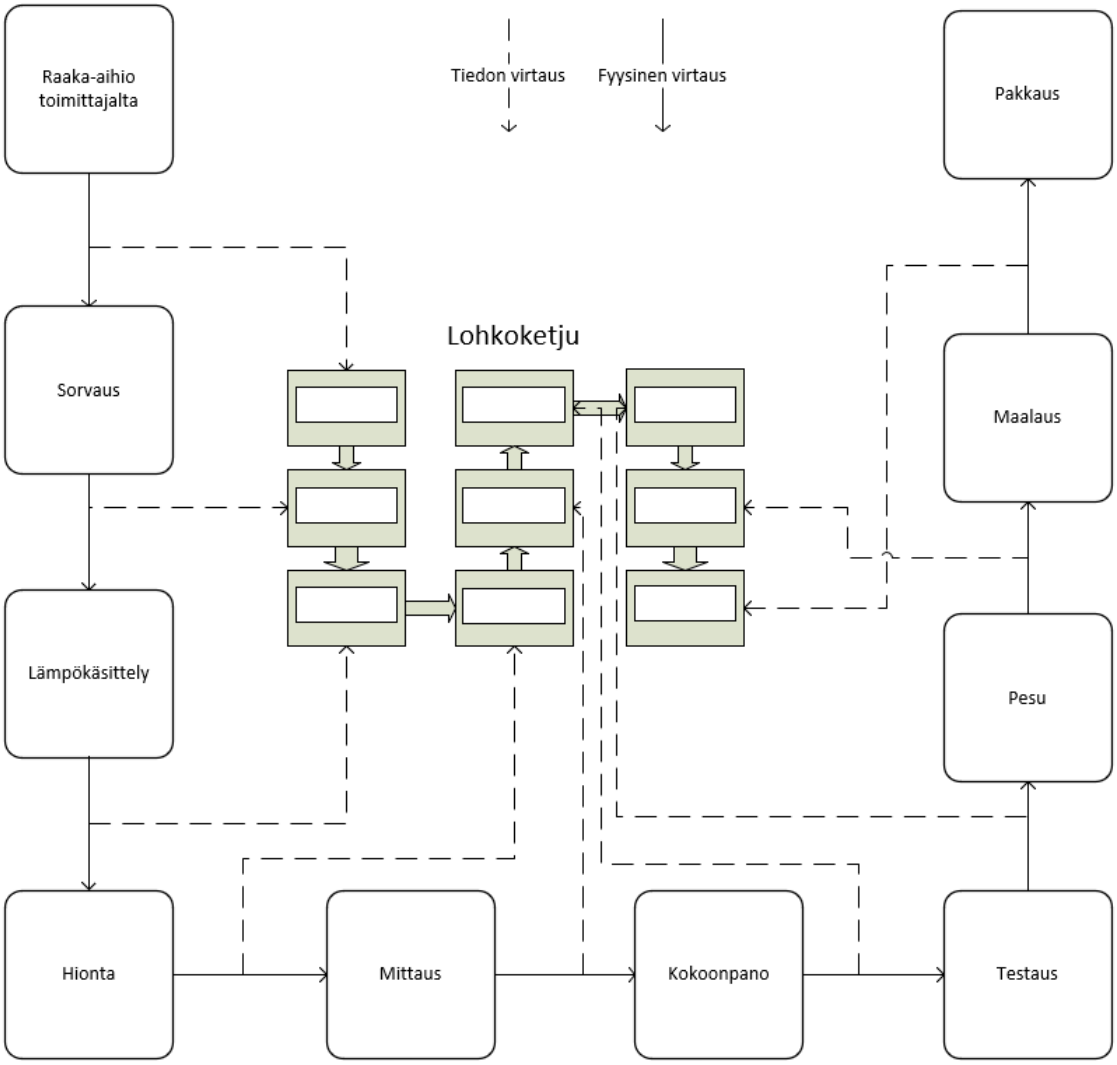
määrätyn käyttäjäjoukon kesken, riski hakkeroinnille kasvaa. [9] Hakkereiden on tällöin helpompi saada kontrolliinsa suurin osa solmukohdista ja ottaa systeemi haltuunsa.

Hybridin lohkoketjun käyttämisellä voidaan hyödyntää julkisen ja yksityisen lohkoketjun parhaat ominaisuudet. Yksityisen lohkoketjun nopeus yhdistettynä julkisen osan tuomalla turvallisuudella mahdollistaa muuttumattomien historiatietojen tallentamisen ilman hakkeroinnin riskiä. [9] Hybridissä lohkoketjussa on mahdollisuus valita, kenellä on oikeus muokata ja tarkastella lohkoketjussa olevia tietoja. Tämä mahdollistaa toimittajien ja asiakkaiden oikeuksien rajaamisen tarvittavilta osin, koska rajattavat tiedot voidaan tallentaa yksityiseen osaan. Lohkoketjun ylläpitäjäryhmän muodostaa toimihenkilöt. Ylläpitäjäryhmälle annetaan täydet oikeudet tarkastella ja muokata lohkoketjun kaikkia tietoja.

4.3 Havainnollistava malli lohkoketjusta

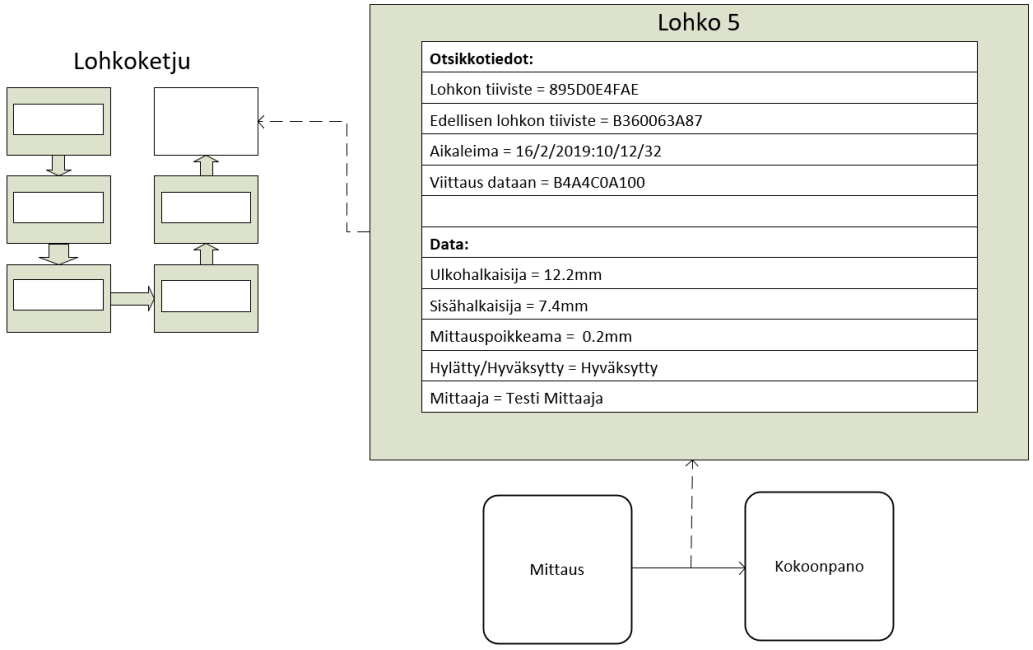
Lohkoketjuteknologia toimitusketjuissa toimii seuraavalla tavalla. Kun tuotteen omistajuus siirtyy osapuolelta toiselle, vain uusi omistaja voi päivittää tuotteen tilaa. Kun uusi omistaja siirtää tuotteen eteenpäin ja päivittää tuotteen tilan, siirrossa tapahtuvista tiedoista muodostetaan lohko. Tässä vaiheessa lohko tallennetaan pysyvästi lohkoketjuun. Jotta tieto saataisiin tallennettua luotettavasti lohkoketjuun, on uuden omistajan hyväksyttävä siirtoon liittyvät tiedot. [25]

Kuvassa 8 on esitetty kuinka eri työvaiheiden väliset siirrot muodostavat aina uuden transaktion lohkoketjuun. Työvaiheista saatava tieto tallentuu transaktion mukana. Lohkoketjuohjelma laskee transaktioille kryptografisen tiivisteen, jolloin lohkot linkittyvät toisiinsa näiden tiivisteiden perusteella. Tiedon virtaus on merkitty kuvaan katkoviivalla ja tuotteiden liikkuminen yhtenäisellä viivalla. Mallin perusidea on tehty sovelluskohteissa esitetyn Mondragonin konferenssijulkaisun [14] perusteella. Siinä käsiteltiin lohkoketjun käyttöä komposiittimateriaalien toimitusketjuissa. Tässä mallissa rajoitetaan tarkastelu yrityksen sisäiseen tuotantoketjuun, eikä huomioida muita osapuolia.



Kuva 8. *Transaktioiden tallennus lohkoketjuun.*

Tarkastellaan tarkemmin mittauksen ja kokoonpanon välillä tapahtuvaa transaktiota. Mittaus on valmistunut, ja on saatu selville kaksi eri halkaisijaa kuvan 9 mukaisesti. Koska mittauspoikkeama on ollut hyväksytyissä rajoissa, kappale on mennyt hyväksytysti läpi. Lohkoon on tallennettu myös mittaajan nimi ja aikaleima. Mittaaja on lukenut kappaleessa olevan QR-koodin, jolla kappale identifioidaan lohkoketjussa. Seuraavaksi kokoonpanovaiheessa oleva käsittelijä hyväksyy transaktion tiedot, jolloin järjestelmä laskee lohkolle muuttumattomat tiivistetiedot, ja lisää lohkon 5 osaksi lohkoketjua.



Kuva 9. *Esimerkkitietojen tallennus lohkoon, ja lohkon lisäys lohkoketjuun.*

Tällä menetelmällä jokainen fyysisesti tapahtuva siirto tallentuu lohkoketjuun mahdollisen datan kanssa. Koska päivitetty kopio lohkoketjusta on jatkuvasti kaikkien oikeuksien omaavien osapuolten nähtävillä, tuotteiden jäljitettävyys ja tuotantoketjun läpinäkyvyys parantuvat. Valmiille tai keskeneräiselle tuotteelle voidaan hakea lohkoketjusta transaktiohistoria, ja seurata kappaleita reaaliajassa.

4.4 Lohkoketjusta saatava hyöty kohdeyritykselle

Lohkoketjuteknologia mahdollistaa prosessien tekemisen läpinäkyvämmäksi ilman kolmannen osapuolen osallistumista. Yrityksen ottaessa lohkoketjun osaksi toimitusketjuaan, laadunvarmistamiseen käytetyt kulut pienenevät lohkoketjuteknologian reaaliaikaisen läpinäkyvyyden ansiosta, ja tuotteiden laadulle löytyy luotettava todiste tarvittaessa. [25] Tuotteiden läpimenoaikojen reaaliaikainen seuranta auttaa ennusteiden tekemisessä ja varastojen pienentämisessä. [Liite A] Lisäykset lohkoketjuun ovat kaikkien oikeuksien omaavien osapuolten nähtävillä samanaikaisesti [7].

Lohkoketjun avulla saadaan parannettua läpinäkyvyyttä ja jäljitettävyyttä kaikkien toimitusketjuun vaikuttavien tahojen kesken. Järjestelmän näkyvyyden parantaminen mahdollistaa ongelmien aikaisemman havaitsemisen, ja toimitusketjun nopeuttamisen ihmisten tekemien päätösten vähentämisellä. [13]

Tuotantovaiheista saatavat tiedot tallennetaan nykyään moneen eri paikkaan, eikä tietoja ole välttämättä helppo löytää jälkeenpäin. Osa tiedoista on pilvipalvelutarjoajien serve-

reillä, osa paikallisesti käyttäjien tietokoneiden kovalevyillä, ja osa saattaa olla vain paperille tallennettuna. Lohkoketjuteknologian käytöllä saavutetaan tietojen helpompi löytäminen ja varmempi säilyminen muuttumattomana. Koska tiedot ovat tallennettuna hajautetusti, yhden solmukohdan hajoaminen ei merkitse tietojen katoamista.

4.5 Jatkokehitysideat

Tämän kandidaatintyön tarkoituksena on tuoda esiin lohkoketjun hyödyntämismahdollisuuksia yrityksen tuotantoketjussa. Tutkimus antaa perustietoa lohkoketjusta ja ehdotuksen sen hyödyntämiselle. Tutkimuksen pohjalta voisi alkaa suunnittelemaan pilottihanketta, johon sisältyisi muutaman tuotteen merkintä, ja tuotteiden elinkaaren seuranta lohkoketjun avulla.

Laajemmin ajatellen lohkoketjun täysi potentiaali saadaan käyttöön vasta, kun mukaan otetaan kaikki toimitusketjun osapuolet toimittajista asiakkaisiin ja huoltoon asti. Aluksi kannattaa kuitenkin tutustua teknologiaan pienemmän hankkeen kautta, koska siirtyminen hajautettuja järjestelmiä käyttävään lohkoketjuun on iso muutos yrityksessä.

5. YHTEENVETO

Tässä kandidaatintyössä käsiteltiin lohkoketjuteknologian hyödyntäminen kohdeyrityksen tuotantoketjussa teoriaselvityksen perusteella. Alussa esiteltiin lohkoketjun toiminnan mahdollistavat tekniikat, joita ovat hajautettuihin systeemeihin perustuvat vertaisverkot. Lohkoketjun päätarkoituksena on eheiden hajautettujen järjestelmien luominen. Lohkoketjut luokiteltiin kolmeen luokkaan, joista yritykselle valittiin hybridi lohkoketju. Hybridi lohkoketju soveltuu parhaiten yrityksen osapuolten käyttöön yhdistäen julkisen ja yksityisen lohkoketjun parhaat puolet.

Sovelluksista tunnetuimpana kerrottiin Bitcoinin toiminnasta. Tutkimuksen kannalta oleellisimpana sovelluskohteena käytettiin komposiittimateriaalien toimitusketju-sovellusta. Siitä saatiin paljon ideoita lohkoketjun hyödyntämismahdollisuuksille yrityksessä.

Tiivistefunktioiden avulla esiteltiin lohkoketjun muuttumattomuutta, ja neljännessä luvussa muodostettiin tuotantovaiheiden välille havainnollistava malli lohkoketjun hyödyntämisestä. Lohkoketjun käytöstä saatava hyöty perustuu läpinäkyvyyden lisäämiseen tuotantoketjussa, jolloin tuotteiden jäljitys helpottuu. Tietojen tallennus kaikkien tarvitsevien osapuolten saataville reaaliaikaisesti on myös lohkoketjun tuoma hyöty.

Tuotteiden lisääminen lohkoketjuun vaatii tuotteiden pysyvän merkinnän. Merkintätavaksi valittiin vertailun perusteella QR-koodi luotettavuuden ja pienen kokonsa ansiosta.

Tarkoituksena oli tehdä laajempi ehdotus lohkoketjun hyödyntämiselle sisältäen käyttöliittymän suunnittelun ja tarkemman mallin. Kandidaatintyön työmäärä ei vastaa näin laajaa tutkimusta, joten nämä jäävät jatkotutkimuksiin. Lisäksi tutkimuksessa ei otettu kantaa toimitusketjun muiden osapuolten saaman hyödyn huomioimiseen.

LÄHTEET

[1] W. Mougayar, V. Buterin, The business blockchain: promise, practice, and application of the next Internet technology, John Wiley & Sons, Inc, Hoboken, New Jersey, 2016.

[2] I. Bashir, Mastering Blockchain, Packt Publishing Ltd, Birmingham, UK, 2017, 531 p.

[3] D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Apress L. P., Berkeley, CA, USA, 2017, 250 p.

[4] P2P, Britannica Academic, Encyclopædia Britannica, 2009. Saatavissa (viitattu 22.11.2018): https://academic-eb-com.libproxy.tut.fi/levels/collegiate/article/P2P/471622

[5] R. Steinmetz, K. Wehrle, Peer-to-Peer systems and applications, Springer, Berlin, 2005, 629 p.

[6] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin Project. Saatavissa (viitattu 17.11.2018): https://bitcoin.org/en/bitcoin-paper

[7] M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, Analysis of Blockchain technology: pros, cons and SWOT, Cluster Computing, 2018, pp. 1–15.

[8] J. Rakheja, What is blockchain? The difference between public and private blockchain, Athena Information Solutions Pvt. Ltd., Gurgaon, India, 2018.

[9] R. Maiya, Public, Private or Hybrid Blockchain: What does it mean?, Dataquest, 2017.

[10] Z. Li, A.V. Barenji, G.Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, ScienceDirect, 2018, pp. 133–144.

[11] Deloitte, Using blockchain to drive supply chain innovation, Deloitte development LLC, 2017. Saatavissa (viitattu 10.2.2019): https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-blockchain-to-drive-supply-chain-innovation.pdf

[12] E. Kinoti, Block chain technology: Benefits and Challenges, Coinweez, 2017. Saatavissa (viitattu 10.2.2019): https://coinweez.com/block-chain-technology-benefits-challenges/

[13] D. Greenfield, Is Blockchain Coming to Manufacturing?, AutomationWorld, 2017. Saatavissa (viitattu 1.2.2019): https://www.automationworld.com/blockchain-coming-manufacturing

[14] A. E. C. Mondragon, C. E. C. Mondragon, E. S. Coronado, Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry, IEEE, International Conference on Applied System Invention (ICASI), 2018, pp. 1300–1303.

[15] A. Kolehmainen, Lohkoketju mullistaa asuntokauppaa Suomessa, Tivi, 2017 Saatavissa (viitattu 2.2.2019): https://www.tivi.fi/Kaikki_uutiset/lohkoketju-mullistaa-asuntokauppaa-suomessa-6693218

[16] T. Lehto, Asuntokauppa tekee digiloikan – varsinkin asuntosijoittaja kiittää, Kauppalehti, 2018. Saatavissa (viitattu 10.1.2019): https://www.kauppalehti.fi/uutiset/asuntokauppa-tekee-digiloikan-varsinkin-asuntosijoittaja-kiittaa/176cdc8a-57bd-4de3-959c-63a45c40acb9

[17] J. Lee, M. Pilkington, How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions], IEEE Consumer Electronics Magazine, Vol. 6, Iss. 3, 2017, pp. 19-23.

[18] R. Ballou, Business Logistics/Supply Chain Management: planning, organizing, and controlling the supply chain, Pearson Prentice Hall, 2004, 789 p.

[19] D. Estampe, Supply chain performance and evaluation models, ISTE, London, England, 2014.

[20] Bar code, Britannica Academic, Encyclopædia Britannica, 2018. Saatavissa (viitattu 10.02.2019): https://academic-eb-com.libproxy.tut.fi/levels/collegiate/article/bar-code/1590

[21] Optiscan, Viivakoodiopas, Optiscangroup, 2019. Saatavissa (viitattu 20.02.2018): https://www.optiscangroup.com/fi/en.php?k=219742

[22] Optiscan, Viivakoodiopas, Optiscangroup, 2019. Saatavissa (viitattu 20.02.2018): https://asiakas.gs1.fi/gs1-yritystunniste/gs1-jarjestelman-ohjeet/9-askelta-viivakoodin-toteutukseen

[23] GS1 Finland OY, 9 askelta viivakoodin toteutukseen, eZ Publish. Saatavissa (viitattu 02.02.2019): https://asiakas.gs1.fi/gs1-yritystunniste/gs1-jarjestelman-ohjeet/9-askelta-viivakoodin-toteutukseen

[24] L. Kubáč, RFID Technology and Blockchain in Supply Chain, Technical University of Ostrava, 2018, pp. 35-44.

[25] T. Ko, J. Lee, D. Ryu, Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings, Sustainability, Vol. 10, Iss. 11, 2018, pp. 4274.

LIITE A: SAVINAISEN HAASTATTELU

Savinaisen haastattelu 10.12.2018

Kenellä olisi oikeus lohkoketjussa olevaan dataan?

Toimittajilla rajalliset oikeudet, eivät voi nähdä kaikkea.

Täydet oikeudet tuotannonjohto, toimihenkilöt, tuotekehitys.

Työntekijöillä rajatut oikeudet, ei kustannustietoja vaan ainoastaan tehtaan sisäinen tieto.

Näiden perusteella valittaisiin hybridi/yksityinen lohkoketju, jossa eri osapuolilla eri oikeudet päästä dataan käsiksi.

Kandiin huomioon otetaan toimittaja ja sisäinen, ettei mene liian laajaksi. Jätetään jatkotutkimuskohteiksi asiakkaan ja huollon kannalta ajattelu.

Mitä pitää ottaa huomioon lohkoketjun kehittämisessä?

Miten lohkoketjuun tallennettua tietoa voidaan hyödyntää, jotta siitä saadaan taloudellista hyötyä. Laatuongelmissa, tuottavuuden parantaminen, osakkeenomistajat, omistajat, asiakastyytyväisyys, varastojen pienentäminen.

Laatukysymykset ja ongelmat, Läpimenoaikojen seuranta.

Missä kappale menee milläkin hetkellä.

Testauksesta saadaan parametreja paljon, jota voi tallentaa lohkoketjuun.

Mittauksessa tallennetaan nykyään dataa, mutta ei tietoa missä se on.

Mitä ongelmia on nykyisessä tuotantoketjussa?

Lohkoketjun kannalta osia ei ole vielä merkitty, joten pitäisi kehittää viivakoodi tai QR. RFID jätetään pois, koska ei koeta tarpeelliseksi. Tarvitsee vain identifioida osa ja data lohkoketjun sisään. Aluksi oli suunnitelmana datan tallennus QR koodiin, mutta ei hyvä, koska ei muualla tallessa sitten.

Suurimpana ongelmana läpinäkyvyyden puute. Kappaleilla saattaa olla monen päivän jaksoja, jolloin ei tiedetä, missä menevät. Olemassa oleva seuranta, Leaniin tallennettuna jokin vaihe etukäteen ja solussa kuitataan kappale vaiheelle.

Mihin tieto on tallennettu nykyään?

Saattaa olla manuaalisesti papereille tallennettuna, pilvipalveluiden tarjoajien servereillä, yksittäisillä kovalevyillä.

Löydetäänkö tuotteen testaaja, jos annetaan 10 vuotta vanhan tuotteen sarjanumero?

Ei löydetä. Saattaisi löytää jotain tiedon osia, jos oikein etsimällä etsisi.