Lasse Tammilehto

LOHKOKETJUTEKNOLOGIAN HYÖDYNTÄMINEN SÄHKÖISTEN POTILASKERTOMUSTEN DATAN HALLINNASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Tammilehto, Lasse
Lohkoketjuteknologian hyödyntäminen sähköisten potilaskertomusten datan hallinnassa
Jyväskylä: Jyväskylän yliopisto, 2021, 34 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja: Halttunen, Veikko

Lohkoketjuteknologia on suhteellisen uusi, laajamittaista kiinnostusta viimeaikoina herättänyt teknologinen innovaatio, joka on tullut alunperin yleisölle tutuksi sähköisen valuuttajärjestelmän Bitcoinin myötä. Lohkoketjuteknologian hyödyntämistä onkin aiemmin tutkittu lähinnä kryptovaluuttojen sekä digitaaliseen talouteen ja rahoitusmaailmaan liittyvien sovellusten osalta. Viimeaikoina ollaan kuitenkin huomattu, että teknologialla on suuri hyödyntämispotentiaali myös laajemmin yhteiskuntaa hyödyttävillä aloilla, joiden toimintaan ei liity rahaa, valuuttaa, kaupankäyntiä, rahoitusmarkkinoita tai muuta taloudellista toimintaa. Tässä tutkielmassa keskitytäänkin tutkimaan lohkoketjuteknologian hyödyntämisen mahdollisuuksia terveydeydenhuoltosektorilla, tarkemmin sähköisten potilaskertomusten hallinnassa. Tutkielman tarkoituksena on kartoittaa aihetta koskevan tutkimuksen nykytilaa ja selvittää, minkälaisia haasteita tällä hetkellä käytössä oleviin sähköisiin potilastietojärjestelmiin liittyy, mitä lisäarvoa lohkoketjuteknologian ominaisuudet voisivat tuoda sähköisten potilaskertomusten hallintaan ja minkälaisia haasteita lohkoteknologian osalta täytyy kuitenkin vielä ratkaista, jotta sen tarjoama potentiaali todella voitaisiin valjastaa hyödyllisellä tavalla. Tutkielmassa selvisi, että nykyiset käytössä olevat potilastietojärjestelmät kohtaavat tiettyjä haasteita ennenkaikkea järjestelmien yhteentoimivuuden, sekä tietojen yksityisyyden ja tietoturvan suhteen. Lohkoketjuteknologian mahdollistamilla hajautuksen, muuttumattomuuden, tarkastettavuuden, läpinäkyvyyden ja salausalgoritmien ominaisuuksilla nähtiin olevan kuitenkin potentiaali ratkaista joitakin potilastietojärjestelmiin liittyviä olennaisia haasteita. Kuitenkin haasteet lohkoketjun skaalautuvuudessa ja varastointikapasiteetin hallinnassa, tietoturvassa ja yhteentoimivuudessa, sekä kulttuurisessa ja sosiaalisessa omaksumisessa todettiin toistaiseksi jarruttavan sen laajamittaista omaksumista. Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielmassä käytetty aineisto on valikoitunut sillä perusteella, miten hyvin se täyttää tieteellisen tutkimuksen kriteerit. Aineiston etsiminen on toteutettu määritellyin hakusanoin eri tieteelisten tutkimusten julkaisukanavista ja tietokannoista.

Asiasanat: lohkoketjuteknologia, sähköinen potilaskertomus, sähköinen potilastietojärjestelmä, hajautettu arkkitehtuuri, terveydenhuolto

ABSTRACT

Tammilehto, Lasse
Utilization of blockchain technology in the management of electronic health record data
Jyväskylä: University of Jyväskylä, 2021, 34 pp.
Information Systems, Bachelor's thesis
Supervisor: Halttunen, Veikko

Blockchain is a relatively new technological innovation that has recently attracted widespread interest and has initially become familiar to the public through the electronic currency system Bitcoin. The utilization of blockchain has previously been studied mainly in cryptocurrencies and in the digital economy and financial world related applications. However, it has been noted recently that technology has great potential in areas that could benefit society at larger scale also, in activities that do not involve money, currency, trade, financial markets or other economic activities. This bachelor's thesis focuses on the possibilities of utilizing blockchain in the healthcare sector, more specifically in the management of electronic health records (EHR). The aim of the thesis is to map the current state of research related to the subject and to find out what challenges are currently associated with electronic health record systems (EHRS), what added value the main features of blockchain technology could bring to electronic health record management and what challenges still need to be addressed in order to truly realize its potential. The study found that current electronic health record systems face certain challenges in terms of system interoperability as well as data privacy and security. In addition, many of these systems are centralized in a single location, which may pose risks, for example in the case of data breaches or natural disasters. However, traditional database systems are still the most commonly used structure in the system architecture of electronic health record systems. The features of decentralization, immutabil-ity, verifiability, transparency, and encryption algorithms enabled by block-chain technology were seen as a possible solution to address some of those key challenges electronic health record systems are facing. However, challenges in blockchain's scalability and storage capacity management, as well as in data security and interoperability, as well as in cultural and social adoption, have so far been identified hampering its larger-scale adoption in this area. This bachelor's thesis has been implemented as a literature review, in which material that meets the criteria of scientific research has been searched from selected databases with selected and defined keywords.

Keywords: blockchain, electronic health record (ehr), electronic health record system (ehrs), decentralization, healthcare

KUVIOT

KUVIO 1 Lohkoketjun rakenne pelkistettynä.....11
KUVIO 2 Keskitetyn ja hajautetun järjestelmäarkkitehtuurin erot.....20

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

SISÄLLYS 5

1 JOHDANTO 6

2 LOHKOKETJUTEKNOLOGIA 9
2.1 Lohkoketjuteknologian perusteet ja pääominaisuudet 9
2.2 Lohkoketjuteknologian hyödyntämisen kehitys 12

3 SÄHKÖINEN POTILASKERTOMUS 14
3.1 Määritelmä 14
3.2 Nykyisten sähköisten potilastietojärjestelmien haasteet 15

4 LOHKOKETJUTEKNOLOGIA JA SÄHKÖISET POTILASKERTOMUKSET 19
4.1 Lohkoketjuteknologian pääominaisuuksien hyödyt 19
4.2 Lohkoketjuteknologian omaksumisen haasteet sähköisten potilaskertomusten datan hallinnan osalta 23

5 YHTEENVETO 27

LÄHTEET 30

1 JOHDANTO

Lohkoketjuteknologia on viime vuosina mielenkiintoa herättänyt uusi ja alati kehittyvä tekniikka, jolla nähdään olevan potentiaali mullistaa ja muuttaa merkittävästi tapaa, jolla tietoja käsitellään. Määritelmänsä mukaan se on omanlaisensa tietokanta, (Dimitrov, 2019) joka pitää sisällään hajautetussa verkossa toimivan, avoimeen lähdekoodiin perustuvan tapahtumarekisterin, joka on matemaattisesti varmennettu, ja johon tallennetut tiedot ovat muuttumattomia (Viitala, 2017). Lisäksi sen kaikki transaktiot tai tapahtumat ovat aikajärjestyksessä, kaikkien osapuolten vahvistamia ja tallennettu niin, että mitään ei voida muuttaa tai väärentää (Viitala, 2017). Nämä sisäänrakennetut ominaisuudet mahdollistavat monenlaisia hyötyjä datan hallinnan suhteen.

Lohkoketjuteknologian hyödyntämistä on aiemmin tutkittu lähinnä kryptovaluuttoihin sekä digitaaliseen talouteen ja rahoitusmaailmaan liittyvissä sovelluksissa. Lohkoketjupohjaisten sovellusten määrä ja sen hyödyntämistavat ovat kuitenkin kasvaneet alun virtuaalivaluutoista myös muihin käyttötarkoituksiin. Nykyään voidaankin tunnistaa lohkoketjun eri kehitysvaiheet, ja ne on tapana jakaa sen kolmeksi eri sukupolveksi tai vaiheeksi, joista käytetään nimityksiä lohkoketju 1.0, lohkoketju 2.0 ja lohkoketju 3.0. (Xu, Chen, & Kou, 2019.) Lohkoketju 1.0, eli lohkoketjuteknologian ensimmäinen sukupolvi koski sen hyödyntämistä lähinnä virtuaalivaluuttojen, pääasiassa Bitcoinin osalta. Bitcoin oli myös ensimmäinen konkreettinen lohkoketjuteknologiaa hyödyntävä sovellus. (Mainelli & Smith 2015.) Lohkoketjun seuraavan vaiheen, eli lohkoketju 2.0 katsotaan alkaneen kun uudenlaiset lohkoketjuteknologian sovellukset mahdollistivat sen käytön (Xu ym., 2019). Näillä lohkoketju 2.0 sovelluksilla tarkoitetaan digitaaliseen talouteen ja rahoitusmaailmaan liittyviä sovelluksia. Juuri käsillä oleva vaihe, jota tutkimuskirjallisuudessa kutsutaan lohkoketjuteknologian kolmanneksi sukupolveksi tai vaiheeksi, pyrkii sen sijaan selvittämään, kuinka kyseistä teknologiaa voitaisiin hyödyntää laajemminkin yhteiskunnallisiin tarkoituksiin, aloilla johon ei liity rahaa, valuuttaa, kaupankäyntiä tai muuta taloudellista toimintaa. Tässä tutkielmassa keskitytäänkin tutkimaan sen hyödyntämispotentiaalia

terveydenhuoltosektorilla. Tarkemmin terveydenhuoltosektorin sisällä aihe on rajattu tutkimaan sen hyödyntämistä sähköisten potilaskertomusten hallinnassa. Sähköisten potilaskertomusten termi on käännetty englannin kielen samaa tarkoittavasta termistä Electronic Health Records (EHR). Lisäksi tutkielmassa puhutaan sähköisistä potilastietojärjestelmistä (engl. Electronic Health Record Systems) Kyseisistä englannin kielen termeistä ei ole olemassa tiettyjä yleisesti määriteltyjä suomen kielen vastineita. Näitä termejä on kuitenkin käytetty käännettynä aiemmin, ja esimerkiksi Mäenpää (2015) käyttää Pro gradu -tutkielmassaan sähköisen potilaskertomuksen ja sähköisten potilastietojärjestelmien käsitteitä viitaten niillä mainittuihin Electronic Health Record- sekä Electronic Helath Record System- termeihin.

Ajan mittaa on huomattu, että nykyiset käytössä olevat potilastietojärjestelmät kohtaavat tiettyjä haasteita järjestelmien yhteentoimivuuden, sekä tietojen yksityisyyden ja tietoturvan suhteen. Lisäksi suuri osa näistä järjestelmistä on keskitetty vain yhteen paikkaan, mikä saattaa aiheuttaa riskejä esimerkiksi tietomurtojen, (kuten nähtiin vastaamo-tapauksessa) tai esimerkiksi luonnonkatastrofien yhteydessä. Silti perinteiset, monesti eri järjestelmien yhteentoimimattomuudesta johtuen epätäydellistä tietoa sisältävät ja fyysisesti yhteen paikkaan keskitetyt tietokantajärjestelmät ovat edelleen yleisesti käytetty rakenne sähköisten potilastietojärjestelmien järjestelmäarkkitehtuurissa. (Miyachi & Mackey, 2021.) Lohkoketjuteknologian replikointimekansimeilla, sekä sen paremmman tietojen yksityisyyden ja tietoturvan mahdollistavilla ominaisuuksilla on merkittävä potentiaali terveydenhuollon alalla, jossa niillä on edellytykset ratkaista joitakin potilastietojärjestelmiin liittyviä olennaisia haasteita. (Ismail, Materwala, & Zeadally, 2019).

Tämä kandidaatintutkielma on toteutettu kirjallisuuskatsauksena, jonka tarkoituksena on kartoittaa aihetta koskevan tämän hetkisen tutkimuksen nykytilaa, ja esitellä aihepiiriin liittyvää keskeistä käsitteistöä. Tutkielmassa pyritään vastaamaan kolmeen tutkimuskysymykseen, jotka ovat:

- Mitkä ovat käytössä olevien tavanomaisten potilastietojärjestelmien suurimmat haasteet?

- Mitä lisäarvoa lohkoketjuteknologia-pohjainen potilastietojärjestelmä voisi tuoda sähköisten potilaskertomusten hallintaan tavanomaisiin potilastietojärjestelmiin verrattuna?

- Minkälaisia haasteita on vielä ratkaistava ennen kuin lohkoketjuteknologiaa voitaisiin todella hyödyntää sähköisten potilaskertomusten hallinnassa?

Tutkielman aineisto on kerätty erilaisista tieteellisten tutkimusten julkaisukanavista. Käyettyjä julkaisukanavia ovat olleet google scholar, jykdok, scopus ja ieee xplore, ja tutkielmassa käytetyt lähteet ovat olleet pääosin

englannin kielisiä. Lähteiden arvioinnissa on käytetty suomalaisen Julkaisufoorumi.fi – sivuston tarjoamaa julkaisukanavahakua, joka arvostelee tieteellisten julkaisujen tieteellisen tason arvioimalla ne 0-3 asteikolla, jossa 1 = perustaso; 2 = johtava taso ja 3 = korkein taso. Tämän lisäksi valinnassa kriteerinä on käytetty julkaisuvuotta; tutkielman lähteiksi on pyritty valitsemaan lähtökohtaisesti uusia ja tuoreita julkaisuja. Vanhempien julkaisujen valinnassa kriteerinä on käytetty viittausten määrää. Lähdeaineiston etsinnässä käytettyjä hakusanoja ja hakusanojen yhdistelmiä ovat pääasiallisesti olleet: ”blockchain”, ”ehr”, ”blockchain ehr”, ”blockchain healthcare”, ”ehr challenges”, ”lohkoketju”, ”lohkoketju terveydenhuolto”.

Tutkielman sisältö on jaettu kolmeen lukuun alun johdannon ja lopun yhteenvedon lisäksi. Ensimmäisessä sisältöluvussa käsitellään lohkoketjuteknologian perusteet; eli mikä se on, miten se toimii ja mitä ominaispiirteitä se pitää sisällään teknologiana. Käsittely rajataan suurimmaksi osaksi datan hallinnan näkökulmaan. Tästä näkökulmasta lähestymällä esitellään, mikä on lohkoketjuteknologia, miten se toimii ja mitä ominaispiirteitä se pitää sisällään teknologiana. Tämän luvun jälkimmäisessä osiossa esittelen aiheen viimeaikaista kehitystä sekä taustaa sille, miten lohkoketjuteknologia on kehittynyt ja kehittymässä sen ensimmäisistä konkreettisista hyödyntämistavoista ja sovelluksista tämän tutkielman aihepiiriä käsitteleviin hyödyntämistapoihin. Käsittelen tätä tutkimuskirjallisuudessa eroteltujen lohkoketjuteknologian kolmen eri sukupolven kautta.

Seuraavassa sisältöluvussa määritellään sähköisen potilaskertomuksen ja sähköisten potilastietojärjestelmien käsitteet. Tämän luvun jälkimmäisessä osassa käydään lisäksi läpi mitä vaatimuksia sähköisten potilaskertomusten asianmukaiseen hallintaan kuuluu ja mitkä ovat käytössä olevien, tavanomaisten järjestelmien olennaisimat haasteet.

Tutkielman kolmannessa sisältöluvussa analysoidaan aluksi, mitä mitä potentiaalisia hyötyjä ja mahdollisia etuja lohkoketjuteknologian pääominaisuudet voivat tuoda sähköisten potilaskertomusten hallintaan. Tämän luvun jälkimmäisessä osiossa käsitellään tutkimuskirjallisuudessa esiin nousseita haasteita ja tekijöitä, jotka vielä jarruttavat lohkoketjuteknologian omaksumista ja käyttöönottoa sähköisten potilaskertomusten ja sähköisten potilastietojärjestelmien osalta.

2 LOHKOKETJUTEKNOLOGIA

Tämän luvun ensimmäisessä alaluvussa esittelen lohkoketjuteknologian perusteet. Keskityn esittelyssä tämän tutkielman näkökulman kannalta lohkoketjuteknologian tärkeimpiin ominaispiirteisiin rajaten käsittelyn suurimmaksi osaksi datan hallinnan näkökulmaan. Tästä näkökulmasta lähestymällä esittelen, mikä on lohkoketjuteknologia, miten se toimii ja mitä ominaispiirteitä se pitää sisällään teknologiana. Toisessa alaluvussa esittelen aiheen viimeaikaista kehitystä sekä taustaa sille, miten lohkoketjuteknologia on kehittynyt ja kehittymässä sen ensimmäisistä konkreettisista hyödyntämistavoista ja sovelluksista tämän tutkielman aihepiiriä käsitteleviin hyödyntämistapoihin. Käsittelen tätä tutkimuskirjallisuudessa eroteltujen lohkoketjuteknologian kolmen eri sukupolven kautta.

2.1 Lohkoketjuteknologian perusteet ja pääominaisuudet

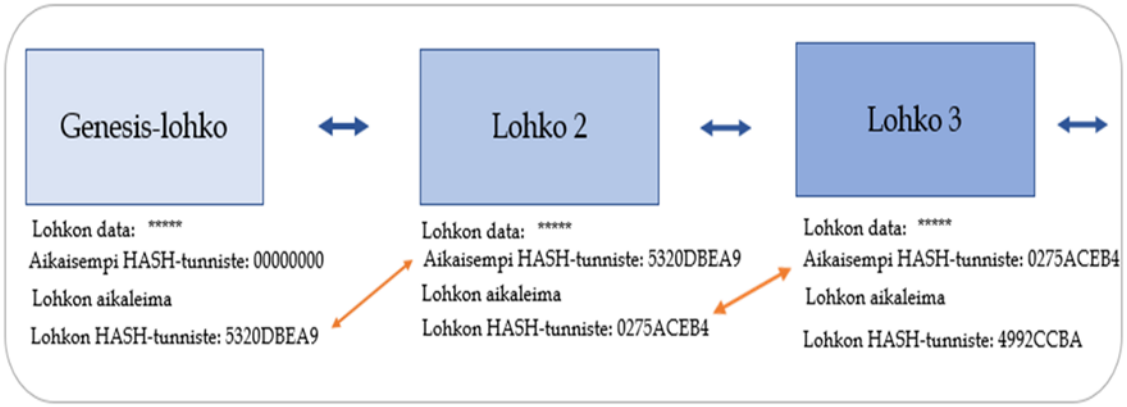
Lokakuussa 2008 tuntematon henkilö joka käytti nimeä Satoshi Nakamoto, julkaisi raportin jossa ensimmäisen kerran johdateltiin yleisö lohkoketjujen maailmaan esittelemällä Bitcoin-niminen sähköinen valuuttajärjestelmä (Hughes, Park, Kietzmann & Archer-Brown, 2019). Bitcoin, jolla on yli 600 miljoonaa suoritettua tapahtumaa (24. helmikuuta 2021) on osoitus siitä, että lohkoketjuteknologia toimii. Toistaiseksi Bitcoin onkin kiistatta yleisimmin tunnettu lohkoketjuteknologian hyödyntäjä. Lohkoketjuteknologia on kuitenkin muutakin kuin pelkkä Bitcoin, ja vaikka Bitcoinin kehittäjä tai kehittäjät samalla kehittivätkin lohkoketjuteknologian perusteet, on teknologialla suuri hyödyntämispotentiaali myös Bitcoinin ulkopuolella useilla muillakin datapohjaisilla aloilla.

Lohkoketjuja on kuvattu eri tavoin. Yleisimmin hyväksytyn määritelmän mukaan ne ovat hajautettuja julkisia kirjanpitoteknologioita (Zhao, Fan & Yan, 2016). Viriyasitavat ja Hoonsopon (2019) määrittelevät ne tutkimuksessaan hieman laajemmin teknologiaksi, joka mahdollistaa sitä käyttävän järjestelmän tietojen muuttumattomuuden ja eheyden, ja jossa järjestelmässä tehtyjen tapahtumien kirjaa pidetään useissa hajautetuissa vertaisverkkoon linkitetyissä

solmuissa. Käytännössä lohkoketjut ovatkin juuri sitä mihin niiden nimi viittaa: transaktioiden tai tapahtumien, ja lohkojen muodostamia pääkirjoja, jotka muodostavat järjestelmällisen, lineaarisen ketjun kaikista koskaan siinä tehdyistä tapahtumista.

Niitä voidaan pitää suunnittelunsa ja määritelmänsä perusteella omanlaisinaan tietokantoina, ja niin myös Dimitrov (2019) määrittelee ne tutkimuksessaan. Yksi keskeinen ero kuitenkin tavallisen tietokannan ja lohkoketjun välillä on tapa jolla tieto on rakentunut. Lohkoketju kerää tietoja yhteisiksi ryhmiksi, eli lohkoiksi, jotka pitävät sisällään tietyn määrän tietoa. Yhdellä lohkolla on tietty tallennuskapasiteetti, tavallisesti yksi kilobitti tai vähemmän per lohko (Dimitrov, 2019). Kun se on täytetty, ne ketjutetaan aiemmin täytettyyn lohkoon ja lohkosta tulee osa ketjua. Tästä prosessista muodostuu ketju dataa, eli nimensä mukaisesti lohkoketju. Kaikki järjestelmään tulevat uudet tiedot, jotka seuraavat edellistä lisättyä lohkoa, kootaan uudeksi muodostetuksi lohkoksi, joka sitten lisätään edelleen ketjuun, kun se on täytetty.

Verrattaessa lohkoketjua tavalliseen tietokantaan, tavallinen tietokanta rakentaa tietonsa taulukoiksi, kun taas lohkoketju, rakentaa tietonsa yhteen ketjutetuiksi lohkoiksi. Tämä tarkoittaa käytännössä sitä, että kaikki lohkoketjut ovat tietokantoja, mutta kaikki tietokannat eivät ole lohkoketjuja. Olennaista on se, että tämä lohkoketjun tapa järjestää tietoa muodostaa luonnostaan peruuttamattoman tietojen aikajanan ja tapahtumaketjun. Kun yksittäinen lohko on täytetty, se on muuttumaton ja siitä tulee osa lohkoketjun aikajanaa. Jokaiselle ketjun lohkolle annetaan tarkka aikaleima, kun se lisätään ketjuun. Kun lohko on lisätty lohkoketjun loppuun, on erittäin vaikea palata takaisin ja muuttaa lohkon sisältöä, ellei enemmistö lohkoketjuverkon solmuista pääse tästä yksimielisyyteen. Tämä johtuu siitä, että lohkoketjut ovat kryptografisesti suojattuja (Yaga, Mell, Roby & Scarfone, 2019). Jokainen lohko sisältää oman hajautuskoodin eli hashin, sen edellisen lohkon hashin sekä aiemmin mainitun aikaleiman (Kuvio 1). Hajautuskoodit luodaan matemaattisella funktiolla, joka muuttaa digitaalisen tiedon merkkijonoksi numeroiksi ja kirjaimiksi. Jos lohkon sisältämiä tietoja muokataan millään tavalla, myös hajautuskoodi muuttuu. Siten kaikki muutokset tietyssä lohkossa tuhoaisivat väistämättä ketjun eheyden, sillä muutokset lohkossa muuttavat samalla sen hash-arvoa. (Yang, Yang, Lei, Zheng & Leung, 2018.)



KUVIO 1 Lohkoketjun rakenne pelkistettynä

Kuo, Kim ja Ohno-Machado (2017) nimeävät tutkimuksessaan lohkoketjuteknologian hyödyllisimmiksi ominaisuuksiksi sähköisen terveysdatan hallinnalle seuraavat ominaisuudet:

- Hajautetun tietojen hallinnan
- muuttumattoman tietojen kirjausketjun
- tietojen alkuperän tarkastettavuuden
- tietojen kestävyyden ja läpinäkyvyyden
- lohkoketjuteknologian salausalgoritmit

Seuraavaksi käyn hieman kutakin ominaisuutta läpi. Ensiksi hajauttaminen. Otetaan esimerkiksi Bitcoin. Kuten tavallinen tietokanta, Bitcoin tarvitsee kokoelman tietokoneita tietojensa tallentamiseksi. Bitcoinille lohkoketju on siis vain tietyntyyppinen tietokanta, joka tallentaa kaikki koskaan tehdyt Bitcoin-tapahtumat. Kuitenkaan Bitcoinin tapauksessa, nämä tietokoneet eivät ole kaikki saman katon alla esimerkiksi yhdessä palvelinkeskuksessa, vaan kukin tietokone tai tietokoneryhmä on hajautettu eri maantieteellisiin sijainteihin ja niitä ylläpitää tavallisesti yksittäiset henkilöt tai henkilöryhmät. Näitä tietokoneita, jotka yhdessä muodostavat Bitcoinin verkon, kutsutaan solmuiksi. Yksi tietokone on yksi solmu ja siinä missä normaali tietokanta on keskitetty usein yhteen pisteeseen, voi lohkoketjun solmuja olla jopa tuhansia. Tästä syntyy lohkoketjuteknologian yksi keskeinen ominaisuus eli hajauttaminen. ”Lohkoketjua ylläpidetään hajautetusti useilla palvelimilla ilman keskitettyä luotettua tahoa, mikä mahdollistaa tiedon säilymisen riippumatta yksittäisestä toimijasta.” (Salonen ym., 2018). Mikään keskusviranomainen kuten pankki tai keskitetyn tietokannan hallinnoija ei myöskään kontrolloi itsessään lohkoketjuun lisättyä sisältöä. Sen sijaan lohkoketjuun välitetyt merkinnät sovitaan jäsenten kesken vertaisverkossa käyttämällä erilaisia konsensusprotokollia. (Hasselgren, Kralevska, Gligoroski, Pedersen & Faxvaag, 2020.) Farouk, Alahmadi, Ghose ja Mashatan esittävät tutkimuksessaan (2020) hyvin havainnollistavan esimerkin tästä vertaamalla lohkoketjun hajautus-ominaisuutta ryhmäviestiin, jossa kaikilla ryhmässä olevilla on kopio viestiryhmän keskustelusta. Tästä seuraa, että jos joku haluaa poistaa jotain pysyvästi ryhmäkeskustelusta, hänen on poistettava se kaikkien ryhmän osaanottajien puhelimesta. Juuri tähän liittyy lohkoketjuteknologian mahdollistaman hajautuksen hyöty. Sen avulla järjestelmä voidaan hajauttaa useisiin solmuihin, jolloin lohkoketjun hajautetun verkon minkä tahansa yhden solmun vaarantuminen ei johda sitä käyttävän järjestelmän tietojen vaarantumiseen, koska sen tiedot toistetaan useassa verkon solmussa. Siinä missä tavanomaiset tietokantajärjestelmät ovat keskitetysti hallinnoituja, on lohkoketju solmujensa kesken hajautettu tietokannanhallintajärjestelmä jossa jokainen solmu toimii itsenäisesti protokolliensa mukaan.

Lohkoketjussa jokaisella sen verkon muodostamalla solmulla on lisäksi täydellinen kirjaus tiedoista, jotka on tallennettu lohkoketjuun sen perustamisesta lähtien. Eli toisin kuin perinteisissä tietokannoissa, lohkoketjun

tapahtumia ei poisteta tai kumota. (Yaga ym., 2019.) Lohkoketjuteknologian yksi tärkeimmistä ominaisuuksista onkin tietojen muuttumattomuus. Esimerkiksi Bitcoinin lohkoketjussa on kaikkien Bitcoin-tapahtumien koko historia. Jos yhden solmun tiedoissa on virhe, se voi käyttää tuhansia muita solmuja vertailupisteenä korjaamaan itsensä. Tällä tavalla yksikään verkon solmu ei voi muuttaa ketjussa olevaa tietoa josta seuraa se, että jokaisen lohkon jotka muodostavat Bitcoinin lohkoketjun, tapahtumahistoria on peruuttamaton. Jos yksi käyttäjä muuttaa Bitcoinin tapahtumarekisteriä, kaikki muut solmut viittaavat toisiinsa ja tunnistavat väärän tiedon omaavan solmun helposti. Muuttumattomuudella tarkoitetaan nimensä mukaisesti lohkoketjun pääkirjan kykyä pysyä muuttumattomana ja koskemattomana. Tästä taas seuraa se, että lohkoketjuteknologian tarjoaman tietojen muuttumattomuuden avulla voidaan varmistaa tietojen eheys. Lohkoketjuteknologian tarjoama tietojen eheys onkin juuri yksi olennaisimmista syistä sille, miksi sen käyttö on laajentunut Bitcoinista myös muihin palveluihin ja sovelluksiin. (Yli-Huumo, Ko, Choi, Park & Smolander, 2016.) Tämä muuttumattomuus-ominaisuus taas tekee lohkoketjuun tallennetuista tietojen alkuperästä helposti tarkastettavia ja tiedoista läpinäkyviä. Nämä ovat niinikään sen tärkeimpiä ominaisuuksia (Hasselgren ym., 2020.) Bitcoinille tämä tieto on luettelo sen tapahtumista ja transaktioista, mutta lohkoketjulla on myös mahdollisuus hallita monia muunkinlaisia tietoja, kuten sähköisiä potilaskertomuksia, johon tässä tutkielmassa erityisesti keskitytään.

Lohkoketjuteknologian viides keskeinen ominaisuus liittyy sen mahdollistamaan potilaskertomusten parempaan tietoturvaan ja yksityisyyteen sen salausalgoritmien ansiosta. Kuo ym., toteavat tutkimuksessaan (2017) kuinka esimerkiksi Bitcoinin lohkoketju käyttää salauksessaan hashina Yhdysvaltain liittovaltion tietojenkäsittelystandardeissa määriteltyä 256-bittistä Secure Hash Algorithm (SHA-256) -salausfunktiota ja epäsymmetristä salausalgoritmia korkean tietoturvan tason luomiseksi.

Pähkinänkuoressa lohkoketjuteknologian tavoitteena on siis mahdollistaa digitaalisen tiedon toimivampi tallentaminen ja jakaminen, mutta estää muokkaaminen. Samalla muiden ominaisuuksien lisäksi myös lohkoketjun salausalgoritmeillä on edellytykset pitää siihen tallennetut tiedot tietoturvallisina.

2.2 Lohkoketjuteknologian hyödyntämisen kehitys

Itsessään lohkoketjuteknologian kehitys onkin ollut progressiivinen prosessi sen julkaisemisesta lähtien. Lohkoketjupohjaisten sovellusten määrä ja sen hyödyntämistavat ovat kasvaneet alun virtuaalivaluutoista myös muihin käyttötarkoituksiin. Nykyään voidaankin tunnistaa lohkoketjun eri kehitysvaiheet, ja ne on tapana jakaa sen kolmeksi eri sukupolveksi tai vaiheeksi, joista käytetään nimityksiä lohkoketju 1.0, lohkoketju 2.0 ja lohkoketju 3.0. (Xu ym., 2019.)

Mainellin ja smithin (2015) mukaan Lohkoketju 1.0, eli lohkoketjuteknologian ensimmäinen sukupolvi koski virtuaalivaluuttojen, pääasiassa Bitcoinin hyödyntämistä. Bitcoin oli myös ensimmäinen konkreettinen lohkoketjuteknologiaa hyödyntävä sovellus. (Mainelli & Smith, 2015.) Tässä ensimmäisessä vaiheessa lohkoketjuteknologiaa käytettiinkin pääosin vain kryptovaluutoissa ja maksujärjestelmissä, jotka tukeutuivat kryptovaluuttaekosysteemeihin (Xu ym., 2019).

Lohkoketjun seuraavan vaiheen eli lohkoketju 2.0 katsotaan alkaneen kun uudenlaiset lohkoketjuteknologian sovellukset mahdollistivat sen käytön (Xu ym., 2019). Lohkoketju 2.0 sovelluksilla tarkoitetaan siis digitaaliseen talouteen ja rahoitusmaailmaan liittyviä sovelluksia. Näitä ovat perinteiseen pankkitoimintaan ja pankkiasiakirjoihin kuten lainoihin liittyvät; monimutkaisiin rahoitusmarkkinavälineisiin kuten osakkeisiin, joukkovelkakirjoihin, futuureihin tai johdannaisiin liittyvät; tai oikeudellisiin asiakirjoihin, kuten omistusoikeuksiin, sopimuksiin ja muihin liittyvät sovellukset. (Efanov & Roschin, 2018.) Rahoitusala edellyttää toiminnassaan korkean tason turvallisuutta ja tietojen eheyttä, ja näihin tarkoituksiin lohkoketjupohjaisilla sovelluksilla onkin paljon annettavaa (Xu ym., 2019). Siinä missä lohkoketjuteknologian ensimmäinen ja toinen vaihe liittyvät ainoastaan kaupankäyntiin ja rahoitusalaan, tarkoitetaan lohkoketju 3.0:lla vaihetta, jossa kyseinen teknologia on levinnyt laajemmin yhteiskunnan hyödynnettäväksi aloille joihin ei liity rahaa, valuuttaa, kauppaa, rahoitusmarkkinoita tai muuta taloudellista toimintaa (Efanov & Roschin, 2018). Lohkoketjun kolmannen vaiheen sovellukset ja hyödyntämiskohteet keskittyvätkin sen hyödyntämiseen muunmuassa tieteessä, taiteessa, koulutuksessa, kulttuurin ja viestinnän eri tarkoituksissa ja muussa julkisen sektorin toiminnassa sekä ennenkaikkea terveydenhuollossa, (Efanov & Roschin, 2018) johon olennaisesti liittyvään osaan, eli sähköisiin potilaskertomuksiin tässä tutkielmassa keskitytään.

3 SÄHKÖINEN POTILASKERTOMUS

Tässä luvussa määrittelen ensiksi sähköisen potilaskertomuksen ja sähköisen potilastietojärjestelmän käsitteen. Tämän jälkeen paneudun käytössä olevien sähköisten potilastietojärjestelmien suurimpiin haasteisiin.

Sähköisten potilaskertomusten termi on käännetty englannin kielen samaa tarkoittavasta termistä Electronic Health Recors (EHR). Lisäksi tutkielmassa puhutaan sähköisistä potilastietojärjestelmistä (Electronic Health Record System.) Kyseisistä englannin kielen termeistä ei ole olemassa tiettyjä yleisesti määriteltyjä suomen kielen vastineita. Kyseistä termiä on kuitenkin käytetty käännettynä aiemmin, ja esimerkiksi Mäenpää (2015) käyttää Pro-gradu tutkielmassaan sähköisen potilaskertomuksen ja sähköisten potilastietojärjestelmien käsitteitä viitaten niillä mainittuihin Electronic Health Record- sekä Electronic Helath Record System- termeihin.

3.1 Määritelmä

Sähköisillä potilaskertomuksilla tarkoitetaan sähköisessä muodossa ylläpidettäviä potilaan terveystietoja, jotka kerätään, luodaan ja tallennetaan sähköisesti (Seymour, Frantsvog & Graeber 2012). Tutkimuskirjallisuudessa sähköisten potilaskertomusten käsitettä ei ole yksiselitteisesti määritelty. International Organization for Standardization määrittelee sen digitaalisessa muodossa ylläpidettäväksi tietovarastoksi, joka mahdollistaa potilaskertomusten tallennuksen ja vaihdannan turvallisesti useiden luvan saaneiden valtuutettujen käyttäjien kesken. Se sisältää tietoja yksilön terveydentilan historiasta, nykyhetkestä ja tulevaisuuden ennusteista ja sen ensisijaisena tarkoituksena on tukea jatkuvuuden, tehokkuuden ja laadun integroimista terveydenhuoltoon. (ANSI, 2005.) Tang ja McDonald (2006) määrittelevät ne lyhyemmin sähköisesti ylläpidettäviksi tietovarastoiksi, jotka sisältävät tiedot potilaan saamasta hoidosta sekä terveydentilasta koko hänen elämänhistoriansa ajalta, ja jotka on tallennettu sillä tavalla, että tiedot ovat

useiden tietoja tarvitsevien ja niihin luvan saaneiden tietovaraston käyttäjien saatavilla ja hyödynnettävissä.

Shahnaz, Qamar ja Khalid (2019) kertovat tutkimuksessaan, kuinka ennen nykyaikaisen tekniikan tuloa terveydenhuoltosektori käytti paperipohjaista ja käsin kirjoittamiseen pohjautuvaa järjestelmää potilaskertomusten tallentamiseksi. Tämä paperipohjainen potilastietojen tallennusjärjestelmä oli heidän mukaansa tehoton, epävarma, organisoimaton ja kohtasi myös tietojen päällekkäisyyttä kun kaikilla eri terveydenhuoltolaitoksilla joilla potilas oli käynyt, oli omat erilaiset kopiot potilaan tiedoista. Lopulta terveydenhuoltoala koki suunnanmuutoksen kun sähköiset potilastietojärjestelmät otettiin käyttöön. Sähköisten potilastietojärjestelmien tavoitteena oli ratkaista paperipohjaisten terveystietojen ongelmat ja tarjota tehokas järjestelmä niiden hallintaan (Shahnaz, Qamar & Khalid 2019).

Sähköisiä potilastietojärjestelmiä onkin otettu käyttöön useissa sairaaloissa ja terveydenhuollon yksiköissä ympäri maailmaa sen sähköisten toimintojen tarjoamien etujen ja hyötyjen vuoksi (Gan & Cao 2014). Näitä toimintoja ovat esimerkiksi potilaskertomusten sähköinen tallennus sekä potilaiden tapaamisten-, laskutuksen- ja laboratoriotestien hallinta (Shahnaz, Qamar & Khalid 2019). Potilastietojärjestelmien perustavoitteena on siis tarjota turvallisia, peukaloinneilta suojattuja sekä helposti eri alustoilla jaettavia ja säilytettäviä lääketieteellisiä asiakirjoja (Shahnaz ym., 2019). Tapurian, Kalran ja Kobayashin (2013) mukaan ne parantavat yksilöiden saaman hoidon laatua ja turvallisuutta, tarjoavat terveydenhuoltopalvelujen ja väestön terveysohjelmien tehostamiseksi tarvittavaa tietoa ja nopeuttaa sekä tehostaa kliinistä tutkimusta ja terveydenhuollon jokapäiväistä toimintaa.

3.2 Nykyisten sähköisten potilastietojärjestelmien haasteet

Tässä alaluvussa esittelen käytössä olevien järjestelmien haasteita keskittyen kahteen tutkimuskirjallisuudessa yleisimmin esiin nousseeseen haasteeseen. Näitä ovat sähköisten potilastietojärjestelmien yhteentoimivuuden haasteet sekä potilastietojärjestelmien tietoturvaan ja tietojen yksityisyyteen liittyvät haasteet.

Kuten aiemmassa luvussa kävi ilmi, terveystietoja on hallittava sähköisesti, jotta niitä voidaan tallentaa, jakaa ja analysoida tehokkaasti. Sähköiset potilaskertomukset tarjoavat kokonaisvaltaisen kuvan potilaan terveydentilasta ja saamasta hoidosta ja niiden avulla voidaan myös analysoida potilasta hoitaneen lääkärin toimintaa. Potilaskertomusten asianmukainen hallinta pitää sisällään kuitenkin tiettyjä vaatimuksia. Ensinnäkin järjestelmiin tallennettavan sisällön on oltava oikeellista ja täydellistä, ja tietojen on oltava jäljitettävissä. Lisäksi niiden tulee pystyä suojautumaan tietojen ei-toivotuilta muutoksilta ja väärentämiseltä. (Durneva, Cousins & Chen, 2020.) Lisäksi potilaiden yksityisyyden ja suojattujen henkilötietojen säilyttämistä koskevien lakisääteisten vaatimusten vuoksi potilaskertomusten on myös oltava

tietoturvallisia ja anonyymisti tallennettavissa järjestelmiin (Durneva ym., 2020). Terveystiedot ovat myös luonteeltaan arkaluonteisia ja henkilökohtaisia, minkä takia niiden säilytykselle on oltava ehkäisymekanismit jotka estävät luvattoman pääsyn tietoihin. Lisäksi tiedot tulisi salata niin, että tietoturvahyökkäyksen tai tietovuodon sattuessa niitä ei voida ymmärtää ilman kryptatun salauksen purkamista. (Durneva ym., 2020.)
Vaikka sähköisten potilastietojärjestelmien oli tarkoitus kehittää ja edistää terveydenhuollon palveluiden laatua ja toimintaa, on niissä sittemmin havaittu tiettyjä ongelmia eivätkä ne ole täysin täyttäneet niihin liitettyjä odotuksia. (Hochman, 2018). Sähköisten potilastietojärjestelmien keskeisimmät haasteet ovat siihen kohdistuvat tietomurrot sekä yhteentoimivuuden ongelmat muiden järjestelmien kanssa (Kumar ym., 2018; Shahnaz ym., 2019).

The National Alliance for Health Information Technology määrittelee järjestelmien yhteentoimivuuden terveydenhuoltosektorin kontekstissa eri tietojärjestelmien ja sovellusalustojen kykynä kommunikoida ja jakaa dataa keskenään tarkasti, tehokkaasti ja johdonmukaisesti, ja kykynä käyttää jaettua dataa (Heubusch, 2006). Yhteentoimivuus terveydenhuoltosektorin kontekstissa voidaan lisäksi jakaa eri kategorioihin joista yksi on sähköisten potilastietojärjestelmien yhteentoimivuus, johon tässä tutkielmassa keskitytään.

Tällä hetkellä erillisten sähköisten potilastietojärjestelmien data on hyvin siiloutunutta, ja näiden lukuisten eri järjestelmien liittämisongelman ratkaisemiseksi on syntynyt laaja valikoima protokollia. Nykyisten protokollien joukossa ei ole kuitenkaan yhtä laajalti hyväksyttyä, joten tiedonsiirto-ongelma on edelleen vakava jokapäiväinen ongelma sähköisissä potilastietojärjestelmissä. (Magyar, 2017.) Sähköisiä potilastietojärjestelmiä on olemassa lukuisia erilaisia, ja niissä käytettävä terminologia, tekniset ominaisuudet sekä käytännölliset ominaisuudet eroavat toisistaan jonka takia yhtä yhteistä protokollaa ei ole pystytty luomaan (Reisman 2017).

Halamka, Lippman ja Ekblaw (2017) toteavat julkaisussaan, kuinka tällä hetkellä potilasta koskevat tiedot joudutaan sovittamaan eri klinikoiden, sairaaloiden, laboratorioiden, apteekkien ja vakuutusyhtiöiden kesken manuaalisella tavalla. Tässä ongelmana heidän mukaansa on kuitenkin se, että ei ole olemassa mitään yhtä koottua listaa siitä, mistä kaikista paikoista data voi olla löydettävissä eikä järjestystä siitä, missä ajallisessa järjestyksessä ne on syötetty. Heidän mukaansa potilasta hoitava taho saattaa siis esimerkiksi tietää jokaisen lääkkeen, joka potilaalle on koskaan määrätty, mutta epäselväksi voi jäädä se, mitä lääkkeitä potilas todella käyttää tällä hetkellä. He toteavat lisäksi, että koska sähköisille potilastietojärestelmille ei ole luotu yhtä yhteistä standardia tai protokollaa, tallentaa jokainen järjestelmä tietonsa käyttämällä omanlaisiaan prosesseja. Tämä saattaa taas johtaa heidän mukaan siihen, että ei ole selvyyttä siitä kuka on tallentanut potilaan tietoja, mitä on tallennettu ja milloin ne on tallennettu.

Durneva ym. (2020) mukaan järjestelmien yhteentoimimattomuus taas tuo esiin erilaisia ongelmia datan hallinnan suhteen. Näitä ovat heidän mukaansa ensinnäkin viiveet tietojen päivityksessä, joka johtaa siihen että tiedot eivät ole

aina tuoreita. Toinen ongelma heidän mukaansa on tietorakenteiden epäjohdonmukaisuus heterogeenisten järjestelmien välillä, joka johtaa siihen että tiedot eivät ole välttämättä eheitä. Kolmas on tietojen läpinäkymättömyys, mikä johtaa siihen että tiedot eivät ole aina välttämättä nopeasti saatavilla, tarkkoja tai oikeellisia. (Durneva ym., 2020.)

Sähköisiin potilastietojärjestelmiin kohdistuu lisäksi paljon tietoturvaloukkauksia (Seh ym., 2020). Toinen sähköisten potilastietojärjestelmien suurimmista haasteista onkin se, kuinka voidaan varmistaa tarpeeksi vahva tietoturva ja yksityisyys sen sisältämien arkaluontoisten tietojen osalta (Seh ym., 2020). Vaikka tietoturva ja tietojen yksityisyys liittyvät vahvasti toisiinsa, Keshta ja Odeh (2020) mukaan niillä tarkoitetaan silti hieman eri asioita. Yksityisyydellä tarkoitetaan heidän mukaansa potilaan oikeutta määritellä, että milloin, miten ja millä laajuudella häntä koskevia henkilökohtaisia tietoja saadaan jakaa tai siirtää toisten käsiteltäväksi. Tietoturvalla taas tarkoitetaan heidän mukaansa sitä, että miltä osin potilaan henkilökohtaisiin tietoihin pääsyä on rajoitettu, ja vastaavasti miltä osin sallittu niihin luvan saaneille henkilöille. Euroopan Unionin tietosuoja-asetuksen 4 artiklan luvussa 12 määritellään henkilötietojen tietoturvaloukkaus:

> Sillä tarkoitetaan sellaista tietoturvaa vastaan kohdistuvaa tekoa, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. (EU:n tietosuoja-asetus 2016/679).

Chernyshev, Zeadally ja Baig (2019) mukaan ohjelmistojen haavoittuvuuksien, muiden tietoturvaongelmien ja inhimillisten virheiden vuoksi luvattomat käyttäjät pääsevät joskus käsiksi sähköisten potilastietojärjestelmien tietokantoihin, jolloin arkaluontoiset potilastiedot altistuvat tietoturvaloukkauksille. Heidän mukaansa tietoturvaloukkaukset voivat tulla myös organisaation sisältä, mikä niin ikään voi johtaa arkaluonteisten terveystietojen menetykseen, varkauteen tai tietojen paljastumiseen. Heidän mukaansa tietoturvaloukkausten kautta saatavat terveystiedot ovat erityisen kiinnostavia siksi, koska niillä on suuri rahallinen arvo pimeässä verkossa. Taloudellinen motiivi onkin yksi suurimmista motiiveista tämän kaltaisiin hyökkäyksiin. Yhtä potilasta koskevan kokonaisen EHR-tietueen arvo voi olla jopa satoja dollareita pimeässä verkossa (Chernyshev, Zeadally & Baig, 2019). Lisäksi koska nämä tietueet voivat sisältää terveystietojen lisäksi sosiaaliturvatunnuksia, kotiosoitteita ja maksutietoja, niitä voidaan laajalti soveltaa myös monenlaiseen muuhun rikolliseen toimintaan (Martin, Martin, Hankin, Darzi & Kinross, 2017).

Seh ym, (2020) esittävät tutkimuksessaan, kuinka vuodesta 2005 vuoteen 2019, terveystietorikkomuksista kärsivien henkilöiden kokonaismäärä oli yhteensä 249,09 miljoonaa, joista 157,40 miljoonaa on tapahtunut pelkästään viiden viime vuoden aikana. Vuonna 2018 tietoturvahyökkäyksiä raportoitiin

yhteensä 2216, 65 eri maassa, ja Näistä terveydenhuollon toimialaan kohdistui 536 rikkomusta. Tämä tarkoittaa, että terveydenhuoltosektori on kohdannut eniten rikkomuksia kaikki toimialat huomioiden (Verizon, 2018). Kokonaismäärä sille, kuinka monta sähköistä potilaskertomusta oli altistunut tietovuodolle, varastettu tai laittomasti paljastettu vuonna 2019, oli 41.2 miljoonaa potilaskertomusta yhteensä 505 niihin kohdistuvassa iskussa. Tietovuotojen voidaan siis todeta olevan todellinen ongelma terveydenhuoltosektorilla ja sähköistenpotilaskertomusten tietoturvallisuuden osalta.

4 LOHKOKETJUTEKNOLOGIA JA SÄHKÖISET POTILASKERTOMUKSET

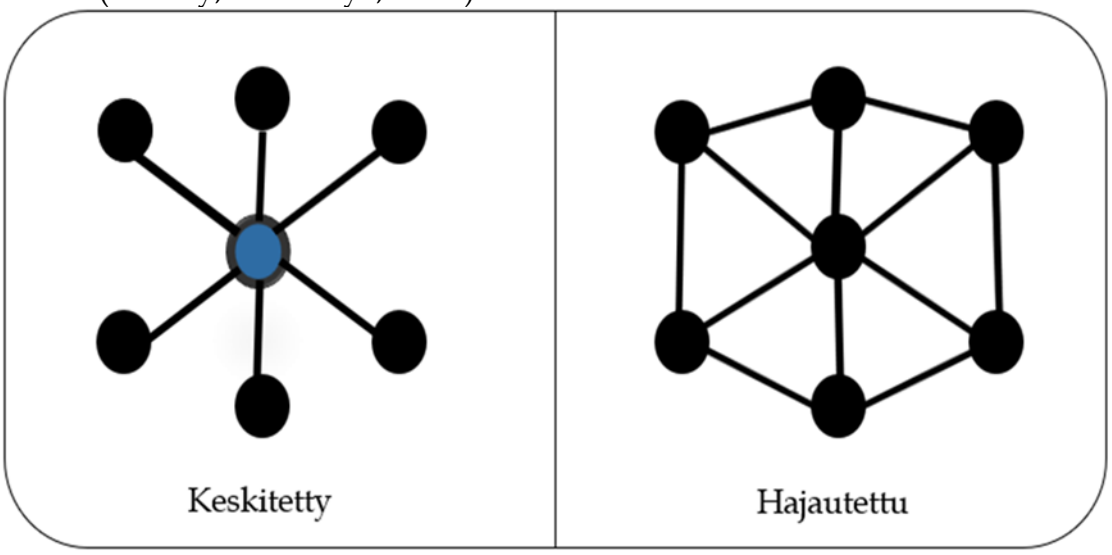
Tässä luvussa käsittelen aluksi lohkoketjuteknologian tärkeimpien ominaisuuksien hyötyjä sähköisten potilaskertomusten hallinnalle. Esittelen myös konkreettiseen käytännön esimerkin ja kerron, kuinka Virossa on otettu ensi askeleet lohkoketjuteknologian hyödyntämisessä tällä alalla. Luvun jälkimmäisessä osiossa käsittelen tutkimuskirjallisuudessa esiin nousseita haasteita ja tekijöitä, jotka vielä jarruttavat lohkoketjuteknologian omaksumista ja käyttöönottoa sähköisten potilaskertomusten ja sähköisten potilastietojärjestelmien osalta.

4.1 Lohkoketjuteknologian pääominaisuuksien hyödyt

Vaikka lohkoketju on merkittävä teknologinen innovaatio, se ei silti väitä olevansa ratkaisu kaikkiin nykyisten sähköisten potilastietojärjestelmien ongelmiin. Pikemminkin lohkoketjuteknologia ottaa nykyisiä järjestelmiä paremmin huomioon tiettyjä olemassa olevia sähköisiin potilastietojärjestelmiin liittyviä ongelmia, joille siihen sisäänrakennetut ominaisuudet voivat tarjota nykyisiä järjestelmiä paremman, tehokkaamman ja turvallisemman alustan. Lohkoketjuteknologia pitää siis sisällään laajan valikoiman hyödyllisiä, siihen sisäänrakennettuja ominaisuuksia joilla on mahdollisuus tuoda tiettyjä hyötyjä sähköisten potilaskertomusten hallintaan. Kuten luvussa 2 todettiin, lohkoketjuteknologian tärkeimpinä ominaisuuksina voidaan pitää sen mahdollistamaa tietojen hajauttamista, tietojen muuttumattomuutta, tietojen alkuperän tarkastettavuutta, tietojen läpinäkyvyyttä ja salausalgoritmeja. (Kuo, Kim & Ohno-Machado 2017.) Käyn seuraavaksi läpi sitä, mitä potentiaalisia hyötyjä kullakin ominaisuudella on mahdollisuutena tuoda sähköisten potilaskertomusten hallintaan.

Ensimmäisenä hajauttaminen. Lohkoketjuteknologian hajautetun arkkitehtuurin mahdollistama tietojen hajautettu tallennus on yksi sen keskeisimmistä ominaisuuksista. Se on myös perusta sille, miksi

lohkoketjupohjaiseen järjestelmään tallennetut tiedot voisivat mahdollistaa paremman tietoturvallisuuden ja tietojen todennuksen verrattuna tavallisiin, keskitettyihin järjestelmiin. (McGhin, Choo, Liu & He, 2019.) Kuten luvussa 2 kävi ilmi, siinä missä tavanomaiset tietokantajärjestelmät ovat keskitetysti hallinnoituja, on lohkoketju solmujensa kesken hajautettu tietokannanhallintajärjestelmä, jossa jokainen solmu toimii itsenäisesti protokolliensa mukaan. Suurin osa terveydenhuoltolaitoksista ja -instituutioista toimii tällä hetkellä keskitetyn järjestelmäarkkitehtuurin pohjalta (Yaqoob ym., 2021). Keskitetyissä järjestelmissä on kuitenkin tiettyjä heikkouksia, ja niistä olennaisin on se, että ne pitävät sisällään niille luontaisen ongelman yhdestä epäonnistumispisteestä (engl. single point of failure) (Pandey, & Litoriya, 2020). Tällä tarkoitetaan sitä, että kun järjestelmä on keskitetty vain yhteen paikkaan, voi tähän yhteen paikkaan kohdistuvat riskit muodostaa merkittävän uhan sen toiminnalle. Esimerkiksi luonnonkatastrofit, tietomurrot sekä tahattomasti tai tahallisesti aiheutetut toimintahäiriöt voivat olla tällaisia tapahtumia. (Pandey, & Litoriya, 2020.) Hajautetussa järjestelmäarkkitehtuurissa, jollaisen lohkoketjuteknologia tarjoaa, on sen sijaan useita verkon koordinaattoreita (Kuvio 2). Jos jotkut verkon koordinaattorisolmut romahtavat, pysyvät yksittäiset solmut silti yhteydessä keskenään edelleen muiden koordinaattorien kautta. (Pandey, & Litoriya, 2020.)



KUVIO 2 Keskitetyn ja hajautetun järjestelmäarkkitehtuurin erot

Hajautettuun arkkitehtuuriin perustuvat verkot kestävät useita vikapisteitä (engl. multiple points of failure), mikä tekee niistä tällöin hyvin vikasietoisia (Rehman 2017). Tästä johtuen lohkoketjuteknologian hyödyntämisellä pystyttäisiin suojelemaan tietoja esimerkiksi mahdollisilta toimintahäiriöiden aiheuttamilta tietojen menetyksiltä, korruptiolta tai ransomware-tyyppisiltä tietoturvahyökkäyksiltä. (Agbo, Mahmoud & Eklund, 2019.) Lisäksi lohkoketjuteknologian hajautus-ominaisuus nähdään mahdollisuutena potilaskertomusten saatavuuden parantamiselle ja mahdollistamaan sellaisten järjestelmien kehittämisen, joissa potilaat voivat hallita itse omia tietojaan aijempaa paremmin (Yaqoob ym. 2021).

Seuraava ominaisuus on lohkoketjuteknologian muuttumattomuus. Kuten toisessa luvussa tuli ilmi, lohkoketju tallentaa ja rekisteröi järjestelmän tapahtumat aikajärjestyksessä digitaalisille lohkoille jotka kukin sisältävät tietyn määrän tietoa ja jotka ovat kukin suojattu hash-salauksella. Kun lohko on lisätty ketjuun, ei sitä pääse enää muokkaamaan. Tämä siis muodostaa toisen lohkoketjun vaikuttavista ominaisuuksista eli muuttumattomuuden. Tietojen muuttumattomuuden hyöty on se, sen avulla voidaan varmistaa tietojen eheys. Alexaki, Alexandris, Katos ja Petroulakis toteavat tutkimuksessaan (2018) että sähköisten potilastietojärjestelmien toimintaympäristö on hyvin monimutkainen. Tästä seuraa, että käytössä olevilla järjestelmillä on haastavaa hallita moninaista lääketieteellistä dataa, ja samalla taata sen pysyminen muuttamattomana. Siinä missä tavalliset järjestelmät mahdollistavat tietojen luomisen, lukemisen, päivittämisen ja poistamisen, mahdollistaa lohkoketju vain luonti- ja lukutoimintoja, mikä tarkoittaa sitä, että siihen tallennettujen tietojen tai tietueiden muuttaminen on erittäin vaikeaa. (Kuo ym., 2017.) Tästä seuraa parempi tietojen eheys. Parempi tietojen eheys taas luo edellytykset sille, että tietoturva ja luottamus tietojen hallintaa kohtaan kasvaa. Kumar, Braeken, Liyanage ja Ylianttila, (2017) toteavat tutkimuksessaan, että tällä hetkellä suurin osa potilaista epäröi jakaa heidän henkilökohtaisia potilaskertomuksiaan tietovuotojen uhan ja mahdollisien tietoturvamekanismien puutteiden vuoksi. Heidän mukaansa hajautetun tietovarastoinnin ja muuttumattoman tietojen kirjausketjun avulla potilaat voisivat varmistua heidän terveystietojensa tietoturvasta ja yksityisyydestä aijempaa paremmin. He toteavat että lohkoketjuteknologia voisi mahdollistaa esimerkiksi sen, että kaikki potilaan tietojen käsittelyyn osallistuvat sidosryhmät sekä potilas itse voisivat saada täydellisen kokonaiskuvan siitä, kuka on hallinnut potilaan tietoja, millä tavalla ja mihin tarkoitukseen. Lohkoketjuteknologian muuttumattomuusominaisuudella pystytään torjumaan sisäisiä tietovuotoja ja tietoturvahyökkäyksiä, sillä kukaan ulkopuolinen kuin lääkärit ja potilaat itse ei voi muuttaa potilaan terveystietoja huomaamatta. (Yue, Wang, Jin, Li, & Jiang, 2016). Muuttumattomus mahdollistaa sen, että lohkoketjuteknologia soveltuu ennenkaikkea kriittisen informaation tallentamisen tarkoituksiin, (Kuo ym., 2017). jollaisia arkaluontoiset potilaskertomukset ovat.

Tietojen alkuperä on myös yksi olennainen ja välttämätön tieto sähköisten potilaskertomusten osalta, jotta tietojen luotettavuudesta pystytään varmistumaan ja sitä pystytään ylläpitämään. Olennaista on hallita, mistä tiedot ovat peräisin, kenellä on oikeus hallita tietoja ja mihin/kenelle niitä on lupa jakaa. (Yaqoob, 2021.) Tavallisessa tietokantajärjestelmässä järjestelmän hallinnoijalla on valta ja mahdollisuudet muuttaa digitaalisten tietojen omistajaa, kun taas lohkoketju luo edellytykset sille, että ainoastaan tietojen omistaja eli potilas itse voi muuttaa tiedon omistusoikeuksia salausprotokollien mukaisesti. Lohkoketju mahdollistaa sen, että tietojen alkuperä ja tietojen alkuperäiset lähteet ovat paremmin varmistettavissa. (McConaghy ym., 2016.) Tämä tarkoittaa, että lohkoketjuteknologian avulla tietojen alkuperää, niihin tehtyjä muutoksia ja tietojen liikettä pystytään seuraamaan. Lisäksi tämä luo

paremmat edellytykset tietojen uudelleenkäytettävyydelle joka on omiaan vähentämään tietojen monisteisuutta. (Yaqoob ym., 2021.)

Läpinäkyvyys on seuraava lohkoketjuteknologian tärkeä ominaisuus. Yaqoob ym., (2021) toteavat, että kun tietojen läpinäkyvyys ja avoimuus otetaan mukaan terveysdatan hallintaan, on mahdollista järjestää täysin tarkastettavissa oleva, oikeellinen ja pätevä potilastietojen ja -tapahtumien kirjanpito. He toteavat myös, että nykyiset terveydenhuollon tiedonhallintajärjestelmät eivät pysty tarjoamaan tietojen yksityisyyttä, turvallisuutta ja avoimuutta samassa paketissa. Lohkoketjuteknologia sen sijaan luo edellytykset näille, sillä se mahdollistaa tietojen paremman läpinäkyvyyden, mutta ei tee sitä yksityisyyden kustannuksella. Agbo ym., toteavat tutkimuksessaan (2019), kuinka se, että lohkoketjuun tallennettu informaatio on replikoitu jokaisen verkon solmun kanssa, luo sekä järjestelmän käytölle läpinäkyvän ja avoimen ilmapiirin, että ottaa huomioon terveydenhuollon eri sidosryhmät osallistavalla tavalla. Heidän mukaansa terveydenhuoltojärjestelmien avoimuudella voidaan mahdollistaa se, että potilaat pysyvät paremmin tietoisina siitä, että miten, missä ja milloin heidän tietojaan käytetään ja on käytetty. Lohkoketjun sisäänrakennetut salausalgoritmit varmistavat sen että läpinäkyvyys pystytään toteuttamaan turvallisella tavalla (Yaqoob ym. 2021). Lohkoketjuteknologian viides keskeinen ominaisuus onkin sen mahdollistama potilaskertomusten parempi tietoturva ja yksityisyys sen salausalgoritmien ansiosta. Kuten luvussa 2 kävi ilmi, käyttää esimerkiksi Bitcoinin lohkoketju salauksessaan hashina Yhdysvaltain liittovaltion tietojenkäsittelystandardeissa määriteltyä 256-bittistä Secure Hash Algorithm (SHA-256) -salausfunktiota ja epäsymmetristä salausalgoritmia korkean tietoturvan tason luomiseksi. (Kuo ym., 2017.) Lohkoketjun data on siis salattua, ja salaus on ainoastaan potilaan itsensä purettavissa yksityisellä avaimella (Dimitrov, 2019). Tästä seuraa, että vaikka haitallinen osapuoli pääsisi tunkeutumaan järjestelmään, ei hänellä ole tapaa päästä käsiksi potilastietoihin (Dimitrov, 2019). Ottaen huomioon terveydenhuoltosektoriin kohdistuneiden tietoturvahyökkäyksien lisääntyvän määrän, sähköisten potilastietojärjestelmien kestokyky niitä vastaan voidaan nähdä tärkeänä seikkana. (Durneva, ym. 2020).

Esimerkiksi Virossa potlaiden sähköiset terveystiedot ovat tallennettu elektronisiin potilasportaaleihin, joissa vain luvanvaraiset valtuutetut henkilöt voivat käsitellä, seurata ja käyttää heidän tietojaan näiden portaalien kautta. (Yaqoob, ym). Viron tapaus onkin mielenkiintoinen ja konkreettinen esimerkki siitä, miten lohkoketjuteknologiaa pystytään, ja on jo pytytty hyödyntämään sähköisten potilaskertomusten hallinnassa. Seuraavaksi tutustummekin tähän tapaukseen hieman tarkemmin.

Vuonna 2016 Viron hallitus etsi uusia ja innovatiivisia tapoja turvata sen 1,3 miljoonan asukkaan potilaskertomukset, ja päätyi lopulta tekemään sen lohkoketjuteknologiaa hyödyntämällä. (Einaste, 2018). Viron hallituksella oli tähän myös oiva kannustin: Vuonna 2007 Viron hallitus joutui massiivisen Venäjältä suuntautuneen valtiollisen kyberhyökkäyksen kohteeksi, mikä oli omiaan halvaannuttamaan Viron hallituksen toimintaa pitkäksikin aikaa.

(Schumacher, 2017.) Tämän johdosta Viron hallitus päätti yhdistää voimansa tietoturvayhtiö guardtimen kanssa, joka on tunnettu lohkoketjuteknologian edelläkävijä. Lohkoketjuteknologian ansiosta Viron uudella järjestelmällä pystytään varmistamaan siihen tallennettujen potilaskertomusten tietojen eheys reaaliaikaisesti, jotta järjestelmänvalvojat pystyvät näkemään mahdolliset tietoturvarikkomukset nopeasti ja reagoimaan niihin välittönmästi estääkseen ja rajoittaakseen niiden aiheuttamia vahinkoja. (Einaste, 2018.) Perinteisen tietoturvakeinojen, kuten palomuurien tapauksessa hyökkäykset voivat jäädä huomaamatta jopa kuukausien ajan, ja on vaikeampi tunnistaa, miten ja mitä tietoja on varastettu tai peukaloitu. (Schumacher, 2017). Ottamalla lohkoketjuteknologian käyttöön Viron hallitus pystyi siis parantamaan sen potilastietojärjestelmän tietojen eheyttä ja tietoturvaa. Virosta onkin tullut ensimmäinen maa, joka on omaksunut lohkoketjuteknologian käytön terveydenhuollossa kansallisessa mittakaavassa.

Olennaista on huomioida se, että viron sähköisessä potilastietojärjestelmässä ei ole lohkoketjun avulla suojattu sähköisiä potilaskertomuksia itsessään, vaan tarkemminkin niiden käsittelyn lokitiedostot, jotka tallentavat kaikki järjestelmän sähköisille potilaskertomuksille suoritetut tietojenkäsittelytoiminnot. Tämän tarkoituksena on turvata arkaluontoiset potilaskertomukset luvattomilta henkilöiltä sekä lieventää kaikkia mahdollisia riskejä tietojen sisäisten ja ulkoisten hakkerointien tai vuotojen varalta. (Einaste, 2018.) Tällä on monia hyötyjä. Lohkoketjuteknologiaan rakennettu loki joka tallentaa kaikki terveystietojen käsittelytoimet pystyy tallentamaan ja aikaleimaamaan jokaisen potilaan sähköisiin tietoja koskevan käsittelyn tai tehdyn muutoksen. Lohkoketjuteknologian kryptografisten hajautustoimintojen avulla pystytään luomaan muuttumaton ja helposti seurattava seurantarata sille, kuka tietoja käsittelee. Sen avulla voidaan myös taata se, että käytössä on aina uusin versio potilaan tiedoista. (Einaste, 2018.) Kaiken kaikkiaan Viron ratkaisun pidemmän tähtäimen visiona on parantaa sen koko terveydenhuoltojärjestelmän kustannustehokkuutta ja kestävyyttä. (Yaqoob, 2021.)

4.2 Lohkoketjuteknologian omaksumisen haasteet sähköisten potilaskertomusten datan hallinnan osalta

Vaikka lohkoketjuteknologian ominaisuuksiin liittyy paljon mahdollisuuksia joilla voi olla hyvät edellytykset parantaa sähköisten potilaskertomusten hallintaa, pitää se sisällään myös monia haasteita ja esteitä, jotka tulee ratkaista ennen kuin sitä voidaan todella hyödyntää ja sen sisältämä potentiaali pystytään todella valjastamaan käytännön toteutuksiksi. Tässä alaluvussa käyn läpi näitä olennaisimpia haasteita.

Ensimmäinen suuri haaste on lohkoketjun skaalautuvuuden ja varastointikapasiteetin hallinnan haasteet. Sähköiset potilastietojärjestelmät sisältävät ja tuottavat valtavia määriä dataa. (Onik, Aich, Yang, Kim & Kim 2019). Lohkoketjuteknologia on kuitenkin alunperin suunniteltu tallentamaan ja

käsittelemään hyvin rajoitetusti tilaa vievää dataa, eli käytännössä dataa kryptovaluuttojen transaktioista, eikä niinkään raskaaseen, paljon tilaa vievään potilaskertomusten tallennukseen. (Esposito, De Santis, Tortora, Chang & Choo, 2018). Kun lohkoketjuteknologia on levittäytynyt ajan myötä terveydenhuoltosektorille, ovat haasteet varastointikapasiteetin hallinnassa käyneet ilmeisiksi. (Siyal ym. 2019). Sähköisten potilastietojärjestelmien on prosessoitava massiivivisia määriä dataa päivittäin potilaiden terveystiedoista ja terveyshistoriasta aina erilaisiin terveyteen liittyviin raportteihin ja röngenkuviin näin esimerkiksi. Kaiken tämän datan on oltava saatavilla jokaisessa lohkoketjun solmussa, joka näin ollen vaatii hyvin suuren määrän tietojen varastointikapasiteettia. (Siyal ym. 2019.) Lisäksi kun lohkoketjupohjaiset järjestelmät ovat transaktiopohjaisia, on lohkoketjupohjaisilla tietokannoilla taipumus kasvaa hyvin nopeasti. Tietokantojen koon kasvaessa tietueiden etsimisen ja saatavuuden nopeus laskee, mikä on hyvin ongelmallista sen tyyppisessä käytössä jossa nopeus on vaatimuksena. Tämän takia lohkoketjupohjaisten potilastietojärjestelmien tulisi olla skaalautuvia ja joustavia. (Siyal ym. 2019.) Skaalautuvuuskysymykseen on kuitenkin esitetty erilaisia ratkaisutapoja. Kim, Kwon, ja Cho, (2018) esittävät että yksi mahdollisista ratkaisuista on niinkutsuttu salamaverkko, jonka tarkoituksena on lisätä toinen kerros ensisijaiseen lohkoketjuverkon päälle, ja näin pyrkiä mahdollistamaan nopeammat transaktiot. Toinen heidän esittämä mahdollinen ratkaisu voisi olla niinsanotun sirpalointitekniikan käyttö, joka auttaa jakamaan transaktioita ikäänkuin sirpaleiksi ja jakamaan ne lohkoketjun solmujen välillä. Tällä tavoin jokaisen solmun ei tarvitse ladata ja tallentaa koko lohkoketjun tilaa, jolloin on mahdollista saavuttaa suuremmat tapahtumanopeudet rinnakkaistamisen kautta (Kim ym., 2018). Yksi mahdollinen ratkaisu on myös käyttää lohkoketjua vain järjestelmän lokitietojen tallentamiseen, kuten nähtiin Viron tapauksessa. Tällä kenties pystytään tiettyyn pisteeseen asti ehkäisemään ketjun datan määrän kasvamista liian suureksi.

Vaikka lohkoketjuteknologian ominaisuuksia voidaan pitää yhtenä potentiaalisena mahdollisuutena nykyisten järjestelmien yksityisyyden ja turvallisuuden, sekä yhteentoimivuuden aiheuttamien haasteiden ratkaisemiseksi, sisältyy siihen omanlaisiaan haasteita myös juuri näiden suhteen. Vaikka oletetaan, että lohkoketju parantaisi koko järjestelmän turvallisuutta, Jo, Khan ja Leen (2018) mukaan lohkoketjupohjaisissa potilastietojärjestelmissä ei ole tarvittavia mekanismeja takaamaan lohkoketjuun sijoitettujen tietojen turvallisuutta. Siyal ym., (2019) toteaa, että lohkoketjun kolmannen osapuolen eliminoiva arkkitehtuuri ei vättämättä takaa aina sitä, että tiedot pysyisivät yksityisinä ja paremmin potilaan hallittavina. He antavat esimerkin tapauksesta jossa potilas valitsee yhden tai useamman edustajan, joka pääsee hänen tietoihinsa ja/tai sairaushistoriaansa käsiksi hänen puolestaan esimerkiksi hätätilanteessa. Nyt tämä potilaan valtuuttama edustaja voi sallia lisäksi joukon muita ihmisiä pääsemään saman potilaan tietueisiin, mikä voi ymmärrettävästi luoda uhan tietoja yksityisyydelle ja turvallisuudelle.

(Siyal ym. 2019). Toisaalta taas Korkean turvallisuuden varmistavien mekanismien sisällyttäminen järjestelmään voi johtaa esteisiin datan siirtämisessä lohkosta toiseen, mikä johtaa siihen että potilasta hoitavan tahon saama tieto voi olla puutteellista ja hyvin rajoitettua. (Siyal ym. 2019.) Yleisemmin tunnettu ongelma tietoturvaan liittyen on lisäksi lohkoketjuverkkojen alttius 51%-hyökkäyksenä tai enemmistöhyökkäyksenä tunnettuille tietoturvahyökkäyksille. Tällä tarkoitetaan tilannetta jossa tietyllä joukolla on hallussa yli 50% lohkoketjun lohkoista mkä johtaa siihen, että he voivat kontrolloida ketjua haluamallaan tavalla ja esimerkiksi estää kaikki uudet ketjun tapahtumat tai transaktiot antamatta niille suostumusta. (Siyal ym. 2019.)

Lohkoketjuteknologia onkin vielä kehittymässä oleva uusi innovaatio, ja siksi se joutuu kohtaamaan haasteita myös kulttuurisen ja sosiaalisen omaksumisen suhteen. Siyal ym., (2019) mielestä on selvää että täysin uudenlaisen ja perinteisistä menetelmistä poikkeavan teknologian omaksuminen ei ikinä käy helposti. Vaikka myös terveydenhuoltosektori on enemmän ja enemmän liikkumassa kohti sen toimintojen laajempaa digitointia, on tunnustettava että sillä on vielä pitkä matka omaksua laajalla mittapuulla lohkoketjun tapainen teknologia, jonka toimintaa ei ole vielä täysin varmistettu kaikkien olennaisten ja huomioon otettavien seikkojen osalta. Kumar ym., (2018) toteaa myös että koska potilastietojen jakaminen ei ole koskaan tapahtunut samalla tavalla useiden osapuolten kanssa niinkuin se tapahtuisi lohkoketjun hajautetussa arkkitehtuurissa, niin sisältyy siihen myös eräänlainen kultturinmuutos-aspekti. Ihmisten käyttäytymisen muuttaminen kohti tietojen jakamista täysin uudella, hajautetulla tavalla voi vaatia siis suurenkin määrän ponnisteluja. Lohkoketjuteknologian alhaisesta omaksumisasteesta voidaan lisäksi päätellä että teknologiaan ja sen sisällään pitämiin menettelytapoihin ei toistaiseksi ainakaan täysin luoteta terveydenhuoltosektorilla (Siyal ym. 2019). Yaqoob ym., (2021) huomauttaa että omaksumista jarruttaa myös osaajapula; tällä hetkellä ei ole tarpeeksi ammattitaitoisia osaajia monimutkaisten vertaisverkkojen hallintaan joten pätevien kehittäjien löytäminen tulee myös osaltaan olemaan yksi ratkaiseva haaste.

On myös todennäköistä että maailman digitalisoituminen ja globalisoituminen synnyttää kasvavan tarpeen globaaleille sähköisille potilastietojärjestelmien ratkaisuille tulevaisuudessa. Onik ym., (2019) nostavatkin tutkimuksessaan esiin näitä globaalin tason haasteita. Heidän mukaansa kansallisen lohkoketjupohjaisen sähköisen potilastietojärjestelmän skaalaaminen globaalille yhteisölle edellyttää kaikesta huolimatta lääketieteellisen tiedon koodaamista koskevien protokollien laajaa hyväksyntää. Tässäkin tapauksessa on huomioitava se tosiasia, että ihmisten ja terveydenhuollon eri toimijoiden sekä eri sidosryhmien kannustaminen tietyllä tapaa täysin uudenlaisen järjestelmän käyttöön on todennäköisesti vaikeaa sekä hyvin kallista.

Onik ym., (2019) näkemyksen mukaan on myös mahdollista että lohkoketjupohjaisten sähköisten terveystietojärjestelmien kehitys noudattaa

samanlaisia suuntaviivoja kuin kryptovaluuttojen. Hän toteaa että kryptovaluuttojen tuleminen alkoi yhdestä ainoasta kryptovaluutasta eli vuonna 2009 tulleesta Bitcoinista. Ajan myötä tilanne johti siihen, että esimerkiksi vuonna 2017 erilaisia kryptovaluuttoja oli jo määrällisesti yli 4300 erilaista. Vaikka tämän kaltainen monimuotoisuus kryptovaluuttojen suhteen on suotavaa, on se mahdollinen sudenkuoppa sähköisten potilastietojärjestelmien kontekstissa kun tavoiteltavana asiana on järjestelmien yhteentoimivuus. Tämä nostaa esiin myös tarpeen mahdolliselle rajat ylittävälle lainsäädännölle ja kansainvälisten standardien luonnille (Gökalp, Gökalp, Çoban & Eren 2018). Kumar ym., (2018) mukaan onnistuminen terveystietojärjestelmien käyttöönotossa edellyttääkin sitä että standardointielinten on määriteltävä asianmukaiset standardit yhteentoimivuuden mahdollistamiseksi. Tällä hän tarkoittaa että lohkoketjuun tallennettujen terveystietojen tapauksessa on tehtävä selvät säännöt esimerkiksi sille, minkä kokoisia ja missä muodossa olevia tietoja voidaan lähettää ja tallentaa lohkoketjuun.

5 YHTEENVETO

Tässä kirjallisuuskatsauksena toteutetussa kandidaatintutkielmassa tutkittiin, kuinka lohkoketjuteknologiaa voidaan hyödyntää sähköisten potilaskertomusten hallinnassa, ja minkälaisia etuja lohkoketjuteknologiaan sisäänrakennetut ominaisuudet voisivat tuoda sähköisten potilaskertomusten hallintaan verrattuna tällä hetkellä käytössä oleviin tavanomaisiin järjestelmiin.

Tutkimuskohteen valinnan motiivina toimi ennenkaikkea aiheen ajankohtaisuus ja uutuus. Lohkoketjuteknologian hyödyntämistä on aiemmin tutkittu lähinnä kryptovaluuttoihin sekä digitaaliseen talouteen ja rahoitusmaailmaan liittyen. Juuri käsillä oleva vaihe, jota tutkimuskirjallisuudessa kutsutaan myös lohkoketjuteknologian kolmanneksi sukupolveksi tai vaiheeksi, pyrkii selvittämään sitä, kuinka kyseistä teknologiaa voitaisiin hyödyntää laajemminkin yhteiskunnallisiin tarkoituksiin, aloilla johon ei liity rahaa, valuuttaa, kaupankäyntiä tai muuta taloudellista toimintaa. Terveydenhuolto onkin juuri tällainen yhteiskunnan sektori, jonka toiminnan merkitys voidaan nähdä lisäksi olennaisen tärkeänä. Terveydenhuoltosektorin sisällä tämän tutkielman aihe rajattiin käsittelemään sen pienempää, mutta jokapäiväisen toiminnan kannalta olennaista osaa, eli sähköisiä potilaskertomuksia. Tutkielmassa pyrittiin siis vastaamaan kolmeen tutkimuskysymykseen, jotka olivat: ”Mitkä ovat käytössä olevien tavanomaisten potilastietojärjestelmien suurimmat haasteet?” ”Mitä lisäarvoa lohkoketjuteknologiaan perustuva potilastietojärjestelmä voisi tuoda sähköisten potilaskertomusten hallintaan tavanomaisiin potilastietojärjestelmiin verrattuna?” Sekä ”minkälaisia haasteita niiden hyödyntämiseen vielä liittyy?”.

Tutkielman alussa käsiteltiin lohkoketjuteknologian perusteet; eli mikä se on, miten se toimii ja mitä ominaispiirteitä se pitää sisällään teknologiana. Käsittely rajattiin suurimmaksi osaksi datan hallinnan näkökulmaan. Tämän luvun jälkimmäisessä osiossa esiteltiin lisäksi aiheen viimeaikaista kehitystä sekä taustaa sille, miten lohkoketjuteknologia on kehittynyt ja kehittymässä sen ensimmäisistä konkreettisista hyödyntämistavoista ja sovelluksista tämän tutkielman aihepiiriä käsitteleviin hyödyntämistapoihin.

Seuraavassa luvussa määriteltiin sähköisen potilaskertomuksen ja sähköisten potilastietojärjestelmien käsite. Luvun jälkimmäisessä osassa käytiin läpi mitä vaatimuksia sähköisten potilaskertomusten asianmukaiseen hallintaan kuuluu ja mitkä ovat käytössä olevien, tavanomaisten järjestelmien olennaisimat haasteet. Vaatimusten osalta selvisi että järjestelmiin tallennettavan sisällön on oltava oikeellista ja täydellistä, tietojen on oltava jäljitettävissä ja pystyä suojautumaan tietojen ei-toivotuilta muutoksilta sekä väärentämiseltä. (Durneva ym., 2020.) Lisäksi vaatimuksena oli, että potilaiden yksityisyyden ja suojattujen henkilötietojen säilyttämistä koskevien lakisääteisten vaatimusten vuoksi sähköisten potilaskertomusten olisi oltava tietoturvallisia ja anonyymisti tallennettavissa järjestelmiin (Durneva ym., 2020). Potilastietojen arkaluonteisuuden vuoksi niiden säilytyksen vaatimuksena oli lisäksi tarvittavat ehkäisymekanismit jotka estävät luvattoman pääsyn niihin. Lisäksi vaadittiin, että nämä tiedot tulisi salata niin, että tietoturvahyökkäyksen tai tietovuodon sattuessa niitä ei voida ymmärtää ilman kryptatun salauksen purkamista. (Durneva ym., 2020.) Sähköisten potilastietojärjestelmien keskeisimmiksi haasteiksi tutkimuskirjallisuuden perusteella nousivat niihin kohdistuvat tietomurrot sekä yhteentoimivuuden ongelmat muiden järjestelmien kanssa.

Tutkielman lopuksi analysoitiin mitä potentiaalisia hyötyjä ja mahdollisia etuja lohkoketjuteknologian pääominaisuudet voivat tuoda sähköisten potilaskertomusten hallintaan. Tärkeimpiä ominaisuuksia tutkimuskirjallisuuden perusteella olivat lohoketjuteknologian mahdollistama hajautettu tietojen hallinta, muuttumattoman tietojen kirjausketju, tietojen alkuperän tarkastettavuus tietojen kestävyys/saatavuus ja läpinäkyvyys sekä lohkoketjuteknologian käyttämät salausalgoritmit. Hajautetun tietojen hallinnan olennaisimpia hyötyjä todettiin olevan sen vikasietoisuus, potilaskertomusten saatavuuden parantaminen ja potilaan omien tietojen paremman hallinnan mahdollistaminen. Muuttumattoman tietojen kirjausketjun olennaisimpia hyötyjä todettiin olevan sen mahdollistama tietojen eheys sekä potilaan parempi kontrolli omien tietojensa yksityisyydestä ja tietoturvasta. Tietojen alkuperän tarkastettavuuden ja tietojen läpinäkyvyyden tuomia olennaisimpia hyötyjä todettiin olevan se, että tietojen oikeellisuudesta, niihin tehdyistä muutoksista ja liikkeistä pystytään varmistumaan aijempaa paremmin. Lisäksi potilastietohuoltojärjestelmien läpinäkyvyydellä voidaan mahdollistaa se, että potilaat pysyvät paremmin tietoisina siitä, miten, missä ja milloin heidän tietojaan käytetään ja on käytetty. Lohkoketjun salausalgoritmi-ominaisuuden hyötynä todettiin se, kuinka sen salauksessaan käyttämä Yhdysvaltain liittovaltion tietojenkäsittelystandardeissa määritelty 256-bittinen Secure Hash Algorithm (SHA-256) -salausfunktio ja epäsymmetrinen salausalgoritmi antaa viimeisen silauksen sähköisen potilastietojärjestelmän tietoturvallisuuden edellytyksille mahdollistamalla sen, että vaikka haitallinen osapuoli pääsisi tunkeutumaan järjestelmään, ei hänellä ole tapaa päästä käsiksi potilastietoihin salausalgoritmien ansiosta. Luvun ensimmäisen osion lopussa esiteltiin myös konkreettinen käytännön esimerkki jossa kerrottiin, kuinka

Virossa on otettu ensi askeleet lohkoketjuteknologian hyödyntämisessä tällä alalla. Luvun jälkimmäisessä osiossa käsiteltiin tutkimuskirjallisuudessa esiin nousseita haasteita ja tekijöitä, jotka vielä jarruttavat lohkoketjuteknologian omaksumista ja käyttöönottoa sähköisten potilaskertomusten ja sähköisten potilastietojärjestelmien osalta. Näitä haasteita olivat ennenkaikkea lohkoketjun skaalautuvuuteen ja varastointikapasiteetin hallintaan liittyvät haasteet, niinikään tietoturvaan ja yhteentoimivuuteen liittyvät haasteet sekä kulttuuriseen ja sosiaalisen omaksumiseen liittyvät haasteet.

Kenties tutkimusaiheen tuoreudesta ja uutuudesta johtuen oli tutkimuskirjallisuudesta selkeästi havaittavissa aiheeseen liittyvän tutkimuksen keskeneräisyys. Lohkoketjuteknologiasta ja sähköisistä potilaskertomuksista löytyy suhteellisen laajalti tutkimuksia, mutta aiheen käsittely niissä liittyy pääosin sitä koskeviin teoreettisiin ja potentiaalisiin mahdollisuuksiin konkreettisten ratkaisuiden sijaan. Lisäksi tieto saattoi olla ajoittain ristiriitaista; lohkoketjuteknologia saatettiin tietyn tutkimuksen mukaan nähdä ratkaisuna esimerkiksi mainittujen yhteentoimivuuden ja tietoturvan haasteisiin, kun taas toisen tutkimuksen mukaan teknologiaa itsessään koskettaa juuri nämä samat haasteet. Jatkotukimuksen osalta ehdottaisinkin tutkimusten kohdistamista aihetta koskevien käytännön toteutusten tutkimiseen ja kehittämiseen. Seuraavaksi olisikin hyvä tutkia sitä, kuinka aiheeseen liittyvä teoreettinen potentiaali ja mahdollisuudet voitaisiin valjastaa konkretiaksi. Tämä edellyttää myös tällä hetkellä monien kehitystä jarruttavien haasteiden ratkaisemista.

LÄHTEET

Agbo, C. C., Mahmoud, Q. H., Eklund, J. M. (2019). "Blockchain Technology in Healthcare: A Systematic Review" Healthcare 7, no. 2: 56.

Alexaki, S., Alexandris, G., Katos, V., & Petroulakis, N. E. (2018). Blockchain-based electronic patient records for regulated circular healthcare jurisdictions. 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

ANSI, I. (2005). ISO/DTR 20514: Health informatics–electronic health record—definition, scope and context.

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43(1), 1-12.

Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. Healthcare informatics research, 25(1), 51.

Durneva, P., Cousins, K., & Chen, M. (2020). The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review. Journal of medical Internet research, 22(7), e18619.

Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. Procedia Computer Science, 123, 116-121.

Einaste, T. (2018). Blockchain and healthcare: the Estonian experience. Retrieved December, 28, 2018.

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing, 5(1), 31-37.

Euroopan Unionin tietosuoja-asetus 2016/679. Annettu Euroopan Unionissa 14.4.2016.

Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223-235.

Gan, Q., & Cao, Q. (2014, January). Adoption of electronic health record system: multiple theoretical perspectives. In 2014 47th Hawaii International Conference on System Sciences (pp. 2716-2724). IEEE.

Gökalp, E., Gökalp, M. O., Çoban, S., & Eren, P. E. (2018). Analysing opportunities and challenges of integrated blockchain technologies in healthcare. In Eurosymposium on systems analysis and design (pp. 174-183). Springer, Cham.

Halamka, J. D., Lippman, A., & Ekblaw, A. (2017). The potential for blockchain to transform electronic health records. Harvard Business Review, 3(3), 2-5.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, 104040.

Heubusch, K. (2006). Interoperability: what it means, why it matters. Journal of AHIMA, 77(1), 26-30.

Hochman, M. (2018). Electronic Health Records: a "Quadruple Win," a "Quadruple Failure," or Simply Time for a Reboot?.

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. Business Horizons, 62(3), 273-281.

Ismail, L. Materwala, H. and Zeadally, S. Lightweight Blockchain for Healthcare. (2019). IEEE Access, 7, 149935-149951.

Jo, B. W., Khan, R. M. A., & Lee, Y. S. (2018). Hybrid blockchain and internet-of-things network for underground structure health monitoring. Sensors, 18(12), 4268.

Ken Miyachi, Tim K. Mackey, hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design, Information Processing & Management,Volume 58, Issue 3,2021,102535,ISSN 0306-4573.

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal.

Kim, S., Kwon, Y., & Cho, S. (2018). A survey of scalability solutions on blockchain. In 2018 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1204-1207). IEEE.

Kumar, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2017). Identity privacy preserving biometric based authentication scheme for naked healthcare

environment. In 2017 IEEE international conference on communications (ICC) (pp. 1-7). IEEE.

Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. (2018). Blockchain utilization in healthcare: Key requirements and challenges. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-7). IEEE.

Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. (2018). Blockchain utilization in healthcare: Key requirements and challenges. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-7). IEEE.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

Magyar, G. (2017). Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In 2017 IEEE 30th Neumann Colloquium (NC) (pp. 000135-000140). IEEE.

Mainelli M, Smith M (2015) Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). J Financial Perspect 3(3):38-58

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358.

McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., ... & Granzotto, A. (2016). Bigchaindb: a scalable blockchain database. white paper, BigChainDB.

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.

Mäenpää, H. L. (2015). Terveydenhuollon tietojärjestelmien arkkitehtuurit ja standardit. pro-gradu tutkielma. Helsingin Yliopisto, tietojenkäsittelytieteen laitos.

Onik, M. M. H., Aich, S., Yang, J., Kim, C. S., & Kim, H. C. (2019). Blockchain in healthcare: Challenges and solutions. In Big data analytics for intelligent healthcare management (pp. 197-226). Academic Press.

Pandey, P., & Litoriya, R. (2020). Securing and authenticating healthcare records through blockchain technology. Cryptologia, 44(4), 341-356.

Rehman, J. (2017). Difference between centralized, decentralized and distributed processing.[Online]Haettavissa osoitteesta:http://www.itrelease.com/2017/11/difference-centralized-decentralized-distributed-processing/

Reisman, M. (2017). EHRs: the challenge of making electronic data usable and interoperable. Pharmacy and Therapeutics, 42(9), 572.

Salonen, J. Halunen, K. Korhonen, H. Lähteenmäki, J. Pussinen, P. Vallivaara, V. Väisänen, T. Ylén, P. (2018). Lohkoketjuteknologian mahdollisuudet ja hyödyt sosiaali- ja terveydenhuollossa - Valtioneuvoston selvitys ja tutkimustoiminta (julkaisusarjan osa 80/2017). Valtioneuvoston kanslia.

Schumacher, A., (2017). Blockchain & Healthcare; 2017 Strategy Guide for the Pharmaceutical Industry, Insurers & Healthcare Providers. https://www.researchgate.net/publication/317936859_Blockchain_Healthcare_- 2017_Strategy_Guide [Accessed 22 01 2019].

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. In Healthcare (Vol. 8, No. 2, p. 133). Multidisciplinary Digital Publishing Institute.

Seymour, T., Frantsvog, D., & Graeber, T. (2012). Electronic health records (EHR). American Journal of Health Sciences (AJHS), 3(3), 201-210.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7, 147782-147795.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3.

Tang, P. C., & McDonald, C. J. (2006). Electronic health record systems. In Biomedical informatics (pp. 447-475). Springer, New York, NY.

Tapuria, A., Kalra, D., & Kobayashi, S. (2013). Contribution of clinical archetypes, and the challenges, towards achieving semantic interoperability for EHRs. Healthcare informatics research, 19(4), 286.

Verizon, V. (2018). Data breach investigations report. 2019G02G15). https://enterprise. verizon. com/resources/reG ports/dbir.

Viitala, J. (2017). Mikä on lohkoketju? Juha Viitala - Lohkoketju. https://juhaviitala.com/2016/12/20/mika-on-lohkoketju/

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. Journal of Industrial Information Integration, 13, 32-39.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial Innovation, 5(1), 1-14.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495-1505.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 1-16.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 1-8.

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue.