Erkka Nurmi

Lohkoketjuteknologian hyödyntäminen terveysalalla

Tietotekniikan kandidaatintutkielma

24. toukokuuta 2017

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Erkka Nurmi

Yhteystiedot: ersanurm@student.jyu.fi

Työn nimi: Lohkoketjuteknologian hyödyntäminen terveysalalla

Title in English: Utilization of Blockchain Technology in the Health Sector

Työ: Kandidaatintutkielma

Sivumäärä: 19+0

Tiivistelmä: Lohkoketjut ja niihin liittyvät älysopimukset ovat uusia teknologioita, joista voi olla suurta hyötyä terveysalalla. Tässä työssä tutustutaan lohkoketjuihin, terveysalan tarpeisiin ja alaa koskevaan relevanttiin lainsäädäntöön. Lisäksi pohditaan mahdollisia tapoja hyödyntää lohkoketjuteknologiaa terveysalan tietojärjestelmän kokonaisarkkitehtuurissa.

Avainsanat: lohkoketju, terveysala

Abstract: Blockchain and smart contracts are a new technology that can be very useful on the health sector. This work examines blockchain, the needs of the health sector and relevant legislation. The work also ponder some ways of utilizing blockchain technology in the overall acrhitecture of the health sector's information system.

Keywords: blockchain, health sector

Sisältö

1 Johdanto

Tutkimuksen tarkoituksena on ottaa selvää, miten lohkoketjuteknologiaa ja siihen liittyviä älysopimuksia voidaan hyödyntää terveydenhuollon sovelluksissa Suomessa. Tämä tehdään määrittelemällä terveydenhuollon tiedonhallinnan tarpeita terveydenhuollon sekä lain näkökulmista ja tämän jälkeen pohtimalla lohkoketjuteknologian soveltumista löydettyihin tarpeisiin ja etsimällä maailmalta jo toteutettuja ratkaisuja.

Sosiaali- ja terveysala on Suomessa juuri kokemassa murrosta ja kiinnostus uusiin teknologioihin on suuri. Tutkimuksen aiheena on tunnistaa sosiaali- ja terveyspalveluihin liittyvät tiedonhallinnon ongelmat ja tarjota niihin mahdollisuuksien mukaan ratkaisuja, jotka hyödyntävät lohkoketjuteknologiaa ja niihin liittyviä älysopimuksia.

Lohkoketjut ovat uusi teknologia, joka tarjoaa useita hyötyjä terveydenhuollon sovelluksiin. Sen tärkeitä ominaisuuksia ovat hajautettu tietorakenne, luottamuksettomuus, tiedon anonyymeys, muuttumattomuus ja tunnistautumisen vaatiminen. Kukin näistä ominaisuuksista tarjoaa suuria hyötyjä arkaluontoisen tiedon tallentamisessa ja käytön seurannassa. Laajaa lohkoketjujen hyödyntämistä vastaaviin palveluihin toteutetaan jo esimerkiksi Virossa.

Tutkimus toteutetaan systemaattisena kirjallisuuskatsauksena, jossa tutustutaan ongelmiin, ratkaisuihin ja teknologiaan. Systemaattinen kirjallisuuskatsaus on tiedekunnassamme perinteinen kanditaatin tutkielman tutkimusmenetelmä ja soveltuu myös tämän aiheen tutkimiseen hyvin.

Tutkielman luvussa Lohkoketjut yleisesti(2) esitellään lohkoketjut ja niiden ominaisuudet suhteessa perinteisiin tiedontallennusmenetelmiin. Siihen, miten lohkoketjut saavuttavat nämä ominaisuudet, perehdytään tarkemmin luvussa Lohkoketjujen ja älysopimusten tekninen toiminta(3). Lohkoketjujen julkisuuden eri tasoja käsitellään alaluvussa Julkiset, yksityiset ja hybridilohkoketjut (3.1) ja eri tapoja toteuttaa lohkoketjuun älysopimusalusta alaluvussa Älysopimusten toteutuksia (3.2). Luku

4 käsittelee lohkoketjujen soveltamista terveydenhuollossa ja tarkastelee sovellettavuuden hyviä 4.1 ja huonoja 4.2 puolia. Luku Lohkoketjuratkaisuja terveydenhuollossa (5) sekä spekuloi mahdollisilla ratkaisuilla (5.1) että tuo esiin jo toteutettuja ratkaisuja (5.2). Tutkielma päättyy yhteenvetoon (6).

2 Lohkoketjut yleisesti

Jotta voidaan puhua siitä, mitä hyötyjä lohkoketjuteknologiasta voi olla sosiaali- ja terveysalalla, on ensin hyvä ymmärtää, mitä lohkoketjut ovat. Tämän luvun sisältö pohjautuu ymmärrykseen lohkoketju- ja älysopimusteknologioiden toiminnasta. Tämän ymmärryksen lähteen toimivat Nakamoto (2008) ja Woods (2014).

Lähtökohtaisesti lohkoketju on tapa tallentaa tietoa. Mikä tekee lohkoketjuista erityisen teknologian ovat sen poikkeukselliset ominaisuudet muihin tiedontallennusmenetelmiin verrattuna. Lohkoketjun merkittäviä ominaisuuksia ovat hajautettu luonne, luottamuksettomuus, vaatimus tunnistautumisesta, anonymiteetti ja muuttumattomuus.

Lohkoketju on hajautettu tietorakenne. Tämä tarkoittaa, että kaikki sen sisältämä tieto on tallennettu usealle eri palvelimelle. Tällaisesta palvelimesta käytetään nimitystä solmu. Hajautuksen etuna on, että tietojärjestelmä on käytännössä immuuni häiriöille ja se pysyy toiminnassa poikkeuksetta.

Hajautukseen liittyy olennaisesti myös lohkoketjujen luottamuksettomuus. Koska tieto on tallennettu kaikkiin solmuihin ja uuden tiedon lisääminen vaatii validifointia kultakin solmulta, käyttäjän ei tarvitse luottaa yksittäisen solmun haltijaan. Lisäksi, koska lohkoketjuun jää jälki kaikista tapahtumista, käyttäjän ei myöskään tarvitse luottaa toisiin käyttäjiin. Sosiaali- ja terveysalalla samaa lohkoketjua voivat käyttää yksittäisen kansalaisten lisäksi sairaalat, yksityiset terveystalot ja monet muut toimijat. Tämän kaltaisessa monen käyttäjän järjestelmässä luottamuksettomuudesta voi olla suurtakin hyötyä.

Tunnistautuminen ja anonymiteetti voivat kuulostaa toisensa pois sulkevilta ominaisuuksilta, mutta näin ei ole. Jokaiseen lohkoketjuun tallennettavaan tapahtumaan liittyy vahva tunnistetieto siitä, kuka tapahtuman on lisännyt. Nämä tunnistetiedot on kuitenkin toteutettu salausavaimia hyödyntäen. Tästä johtuen tapahtumaa tarkastelemalla ei voida nähdä kuka sen on lisännyt. On kuitenkin mahdollista näyttää todeksi, että tietty henkilö on lisännyt tietyn tapahtuman. Tapahtumat

sosiaali- ja terveysalan lohkoketjussa voisivat tarkoittaa esimerkiksi kirjautumisia järjestelmään, suostumuksen antamista hoitoon tai reseptin antamista.

Lohkoketjuihin tallennettu tieto on muuttumatonta. Lohkoketjun lohkot koostuvat halutuista lisättävistä tiedoista ja linkistä edelliseen lohkoon. Näin uudet lohkot sidotaan vanhoihin, eikä edellisten lohkojen tietoja voida enää muuttaa uudempia muuttamatta.

3 Lohkoketjujen ja älysopimusten tekninen toiminta

Nakamoto (2008) kuvaa lohkoketjun yleistä toimintaa. Lohkoketju koostuu nimensä mukaisesti joukosta toisiinsa ketjutettuja lohkoja. Kukin lohko koostuu edellisen lohkon tiivisteestä, tallennettavasta tiedosta ja mahdollisesta toiminnan vaatimasta tiedosta, kuten nonce-numerosta.

Kuten Nakamoto (2008) kertoo, lohkoketjua ylläpitää joukko solmuja. Nämä ovat palvelinkoneita, joille kullekkin on tallennettu kopio koko lohkoketjusta. Solmu kerää joukon käyttäjien luomia tapahtumia eli transaktioita ja tarkistaa niiden oikeellisuuden. Kun solmulla on riittävä määrä oikeellisia transaktioita, se luo niiden pohjalta uuden lohkon ja lähettää sen muille solmuille. Muut solmut tarkistavat myös tietojen oikeellisuuden ja ottavat uuden ketjun käyttöönsä.

3.1 Julkiset, yksityiset ja hybridilohkoketjut

Koska solmut hallinnoivat lohkoketjua, on lohkoketjun käytön kannalta erittäin tärkeää, kuka hallinnoi solmuja. Eri lohkoketjuratkaisujen solmujenluontimallit voidaan jakaa kolmeen ryhmään. Nämä ovat julkiset lohkoketjut, yksityiset lohkoketjut ja hybridi-/konsortiolohkoketjut.

BitCoin(Nakamoto (2008)) sekä Ethereum(Woods (2014)) ovat molemmat toteutettu julkisina lohkoketjuina. Näissä kuka vain haluava voi luoda lohkoketjuun uuden solmun. Julkiseen lohkoketjuun tallennettu tieto onkin siis julkista, joskin kryptografisesti salattua. Julkisissa lohkoketjuissa on vaarana, että solmut luovat ja hyväksyvät vain itselleen suotuisia lohkoja. Tämän estämiseksi uusien lohkojen lisäämistä on keinotekoisesti vaikeutettu. Nakamoto (2008) käyttää tähän Proof-of-work -metodia. Proof-of-work vaatii, että uuden lohkon on täytettävä laskennollinen ehto, joka perustuu edellisen lohkon tietoihin. Solmut hyväksyvät valideista ketjuista pisimmän, joten kilpailevien ketjujen luominen ei ole taloudellista. Parhaimman hyödyn solmun ylläpitäjä saa täten toimimalla rehellisesti.

Yksityisessä lohkoketjussa kaikki solmut ovat yhden toimijan hallinnassa. Tämä tarkoittaa, että myös koko lohkoketju on kyseisen toimijan hallinnassa ja toimija pystyy halutessaan muuttamaan lohkojen sisältöä. Yksityinen lohkoketju siis vaatii käyttäjien luottamuksen ylläpitävää tahoa kohti. On merkittävää huomata, ettei yksitynen lohkoketju eroa toiminnaltaan kovin merkittävästi perinteisestä yksittäisen tahon ylläpitämästä tietokannasta. MultiChain on esimerkki yksityisten lohkoketjuratkaisujen tarjoajasta (citeMC).

Hybridi- eli konsortiolohkoketjut ovat lohkoketjuja, joiden solmuja ylläpitää joukko valikoituja toimijoita. Hybridilohkoketjujen konsensusmenetelmät voivat poiketa toisistaan paljonkin, kuten myös Swanson (2015) toteaa.

3.2 Älysopimusten toteutuksia

Lohkoketjuista puhuttaessa tulee vastaan usein myös älysopimuksen käsite. Älysopimus on ohjelma, joka suoritetaan tapahtuman lohkoketjuun kirjaamisen yhteydessä. Älysopimusalusta voidaan luoda lohkoketjuun usein eri tavoin. Tässä selitetään näistä kolme, jotka ovat älysopimusten toteuttaminen transaktiotulosteiden avulla, tapahtuman toimiminen herätteenä älysopimusverkolle ja älysopimusten toteuttaminen sidosketjuissa.

3.2.1 Älysopimusten toteuttaminen transaktiotulosteiden avulla

Transaktiolla tarkoitetaan lohkoketjuista puhuttaessa sellaista tapahtumaa, josta jää jälki lohkoketjuun. Bitcoinin tapauksessa nimike on osuva, koska tällaiset tapahtumat ovat arvon eli bitcoinien siirtoa käyttäjien välillä. Nakamoto (2008) kuvaa, miten Bitcoinin kunkin transaktion arvo koostuu syötteistä, jotka kyseinen transaktio kerää sitä edeltäneiden transaktioiden tulosteista. Tätä voi verrata todellisessa maailmassa siihen, että henkilö kerää yhteen hänelle kertyneitä kolikoita ostaakseen niillä jotain. Käyttämättömistä tulosteista käytetään nimitystä UTXO (Unspent Transaction Output) (Buterin (2014)).

Buterin (2014) huomauttaa, että järjestelmää, jota Bitcoin käyttää transaktiotulos-

teiden käyttäjän varmistamiseen, voidaan käyttää myös muunlaisten ehtojen luomiseen. Kuten Buterin (2014) kirjoittaa, kullakin transaktiotulosteella on ehtoja, jotka kyseisen tulosteen syötteenä käyttävän transaktion on toteutettava. Näiden ehtojen alkuperäinen tarkoitus on toimia varmistuksena siitä, että seuraavan transaktion voi tehdä vain henkilö, jolle rahat kuuluvat. Ehtojen kirjoittamiseen käytettävällä kielellä UTXO:hin saa myös liitettyä yksinkertaisia älysopimuksia, jotka rajoittavat, miten ja milloin tulosteen sisältämän arvon voi käyttää.(Buterin (2014))

Tällaiset älysopimukset ovat kuitenkin varsin rajoittuneita. Kuten Buterin (2014) ja Bitcoinwiki (2017) toteavat, Bitcoinissa näiden skriptien kirjoittamiseen käytettävä kieli ei ole Turing-täydellinen, eikä siis pysty toteuttamaan kaikkia kuviteltavia sopimuksia. Vastaavalla tavalla transaktiotulosteisiin rakennettu älysopimusalusta voisi toki käyttää Turing-täydellistä kieltä, mutta Buterin (2014) nostaa esille myös muita ongelmia. Ensinnäkin transaktiotulosteeseen sidottu älysopimus on sidottu myös transaktiotulosteen arvoon, joten tällaisella alustalla on vaikeaa toteuttaa sopimuksia, joiden arvo voi vaihdella. Käytännössä vaihtelevan arvon sopimuksen saisi toteutettua vain luomalla useita rinnakkaisia ja eriarvoisia sopimuksia. Toinen suuri ongelma tämän kaltaisissa sopimuksissa on, että transaktio tuloste voi olla joko käytetty tai käyttämätön, eikä näin salli vaiheittaisten tai useampitilaisten sopimusten luomista.

3.2.2 Älysopimusten toteutteminen älysopimusverkoissa

Ethereum-älysopimusalusta on toteutettu virtuaalikoneella toimivien älysopimusverkkojen avulla (Woods (2014)). Buterin (2014) kuvaa älysopimusverkon koostuvan useista tileistä. Näitä tilejä on kahdenlaisia. Tileistä, jotka kuuluvat tietylle käyttäjälle tai muulle tiivisteavaimen haltijalle, käytetään tässä tekstissä nimitystä avaintili. Muista tileistä, eli niistä, joita kukaan verkon ulkopuolinen ei hallitse, käytetään tässä nimitystä sopimustili. Buterin (2014) selittää kunkin tilin sisältävän tiedon tilille kuuluvasta kryptovaluutasta ja sen määrästä, nonce-numeron transaktioiden ainut kertaisuuden varmistamiseksi, sopimuskoodin ja sopimuksen käyttämän tallennustilan.

Avaintilit lähettävät älysopimusverkkoon transaktioita, jotka tallennetaan lohkoketjuun ja toimivat herätteinä sopimustileille. Herätteen saatuaan sopimustilit tekevät itseensä herätteen edellyttämät muutokset ja lähettävät tarvittaessa herätteenä toimivan viestin muille sopimustileille.(Buterin (2014)) Vain transaktiot tallennetaan lohkoketjuun, koska sopimustilien väliset viestit ovat deterministisiä.

3.2.3 Älysopimukset sidosketjuissa

Jos tietty lohkoketju todetaan huonoksi alustaksi älysopimuksilla, voidaan se sidostaa toiseen paremman alustan tarjoavaan ketjuun. Tämä voidaan tehdä niin sanotun kaksisuuntaisen sidoksen avulla. Kaksisuuntainen sidos saadaan luotua lukitsemalla kahden lohkoketjun kryptovaluutan arvo toisiinsa ja tarjoamalla tapa siirtää arvoa ketjujen välillä. (Back, Corallo, Dashjr, Friedenbach, Maxwel, Miller, Poelstra, Timón & Wuille (2014))

Backin ym. (2014) mukaan arvon siirtäminen saadaan toteutettua seuraavasti. Käyttäjä lähettää pääketjun valuuttaa tilille, jossa se pysyy lukittuna ja käyttökelvottomana. Tämän jälkeen käyttäjä todistaa sidosketjun louhijalle lukinneensa arvon ja louhija antaa käyttäjän käytettäväksi sidosketjun valuuttaa. Tavasta, jolla arvon lukitsemisen voi todistaa käytetään nimitystä proof-of-burn. On huomattava, että arvon siirtäminen ketjujen välillä vaatii käyttäjän luottamusta louhijaan.

4 Lainsäädännön vaatimukset

Laki rajoittaa tapoja, joilla lohkoketjuja voidaan Suomessa hyödyntää terveydenhuollossa. Toisaalta laki myös antaa vaatimuksia, joiden täyttämiseen lohkoketjut sopisivat hyvin. Keskeisiä aihetta koskevia lakeja ovat Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (L 159/2007) ja Laki potilaan asemasta ja oikeuksista (L 785/1992).

4.1 Lohkoketjujen hyödyt lain näkökulmasta

Laki asettaa tarkat vaatimukset sosiaali- ja terveysalan asiakastietojen tallennukselle. Lohkoketjuteknologia vastaa useaan näistä paremmin, kuin muut tiedon tallentamisen menetelmät. Keskeisiä vaatimuksia, jotka lohkoketjuteknologia täyttää hyvin, ovat tunnistautuminen ja käytönseuranta, oikeuksienhallinta sekä luotettavuus.

Tunnistautumisesta ja käytönseurannasta laki sanoo "[a]siakastietojen sähköisessä käsittelyssä asiakas, sosiaalihuollon ja terveydenhuollon palvelujen antaja, muu asiakastietojen käsittelyn osapuoli ja näiden edustajat sekä tietotekniset laitteet tulee tunnistaa luotettavasti"(L 159/2007, 8 §). Lisäksi "[p]alvelujen antajan tulee kerätä asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja jokaisesta asiakastietojen luovutuksesta seurantaa varten lokitiedot lokirekisteriin"(L 159/2007, 5 §). Lohkoketju täyttää nämä vaatimukset hyvin. Käyttäjän on aina käytettävä vahvaa tunnistautumista lohkoketjutapahtuman luomiseksi ja kuhunkin tapahtumaan lohkoketjussa jää jälki sen luojasta. Vastaavasti täyttyisi myös vaatimus sähköisistä allekirjoituksista (L 159/2007, 9 §, 12 §), jotka voitaisiin toteuttaa lohkoketjutapahtumina.

Lain mukaan "[s]osiaalihuollon ja terveydenhuollon palvelujen antajan tulee pitää rekisteriä omien asiakastietojärjestelmiensä ja asiakasrekisteriensä käyttäjistä sekä näiden käyttöoikeuksista"(L 159/2007, 5 §). Tämä vaatimus saataisiin toteutettua melko yksinkertaisesti portinvartioina toimivien älysopimusten avulla. Nämä älysopimukset voisivat tarkistaa lohkoketjusta onko käyttäjällä oikeudet suorittaa toi-

minto, jota hän on yrittää suorittaa. Käyttöoikeuksista saataisiin pidettyä kirjaa luomalla lohkoketjuun tapahtuma kullekkin käyttöoikeusmuutokselle.

Lohkoketjut ovat hajautettuina järjestelminä lähes immuuneja toimintahäiriöille. Näin lohkoketjut toteuttavat erinomaisesti lain vaatimuksen siitä, että "[v]altakunnallisten tietojärjestelmäpalvelujen ja potilastietojen tulee olla käytettävissä ympärivuorokautisesti"(L 159/2007, 16 §).

4.2 Lohkoketjujen heikkoudet lain näkökulmasta

Lakiin on kirjattu myös vaatimuksia, joita lohkoketjuteknologia ei voi täyttää. Useat näistä liittyvät lohkoketjujen hajautettuun luonteeseen ja tiedon pysyvyyteen.

Yksi suuri ongelma lohkoketjuissa on, että ne ovat hajautettu tietorakenne. Lain mukaan "[p]otilasasiakirjoihin sisältyvät tiedot ovat salassapidettäviä"(L 785/1992, 13 §). Tämän on tarkennettu tarkoittavan, että potilasasiakirjoja ei saa antaa sivullisille. Lohkoketju ei ole henkilö, mutta tiedon säilyttäminen sen kaltaisessa hajautetussa järjestelmässä voi olla ongelmallista. Lohkoketjuteknologiaa voidaan toki myös hyödyntää siten, ettei se toimi varsinaisen potilastiedon varastona.

Edelliseen liittyvä vaatimus on se, että "[s]ähköisestä asiakasasiakirjasta tulee olla vain yksi alkuperäinen tunnisteella yksilöity kappale"(L 159/2007, 4 §). Lohkoketjun hajautus on tässäkin ongelma. Vaikkei varsinaisia potilastietoja säilytettäisikään lohkoketjussa, tämä vaatimus estänee myös sähköisten allekirjoitusten toteuttamisen lohkoketjuja hyödyntäen.

Lohkoketju on pysyvä tietorakenne. Tieto, joka tallennetaan lohkoketjuun, pysyy siellä, kunnen jokainen lohkoketjun solmu lakkaa olemasta. Lain mukaan "[p]otilasasiakirjat, näytteet ja mallit tulee hävittää välittömästi sen jälkeen, kun niiden säilyttämiselle ei ole edellä tarkoitettua perustetta"(L 785/1992, 12 §) ja "[a]siakastietojen käyttäjien käyttöoikeustiedot ja lokitiedot tulee hävittää, kun ne eivät enää ole tarpeen asiakastietojen käytön ja luovutuksen lainmukaisuuden seuraamiseksi"(L 159/2007, 5 §). Tämä ei yksinkertaisesti ole mahdollista lohkoketjuja käytettäessä. Loh-

koketju on pysyvä tietorakenne ja tiedon poistaminen siitä vaatisi koko lohkoketjun tuhoamista.

Laissa myös säädetään, että "[k]ansaneläkelaitos pitää yllä potilaan tiedonhallintapalvelua"ja siihen liittyvää rekisteriä (L 159/2007, 14a §). Tälläkin tavoin lohkoketjuja voitaisiin hyödyntää, mutta se ei välttämättä ole järkevää. Lohkoketju on sitä vahvempi, mitä useampi solmu siinä on. Olisi siis ehkä kannattavaa luoda konsortiolohkoketju, jonka solmuja voisivat ylläpitää Kelan ohella myös sairaalat, vakuutusyhtiöt, kunnat ja muut vastaavat toimijat.

5 Lohkoketjuratkaisuja terveydenhuollossa

Meille on nyt selvillä lohkoketjujen toiminta ja lain määräykset koskien terveydenhuollon tietorakenteita. Voimme siis ryhtyä tarkastelemaan, miten lohkoketjuja voitaisiin hyödyntää terveysalalla.

5.1 Lohkoketjun mahdollinen paikka laajemmassa arkkitehtuurissa

Lohkoketjuteknologian hyödyntämisen kannalta pidän tärkeänä määrittää järjestelmästä neljä eri elementtiä. Ensinnäkin *tietokanta* on järjestelmän pääasiallinen tiedon tallentamiseen tarkoitettu väline. Se sisältää kaikkien asiakkaiden asiakastiedot ja kaiken muun järjestelmän tarvitseman säilytettävän tiedon. Toisekseen *tiedonkäsittely* on kokoelma menetelmiä, joilla tietoa käsitellään. Se käsittelee sekä tietokannassa olevia tietoja että käyttäjien syötteitä ja hoitaa tiedon tallentamisen tietokantaan. Kolmanneksi *käytönseuranta* valvoo kaikkea käyttäjien tiedonkäsittelylle viemää tietoa. Se voi myös valvoa osaa tiedonkäsittelyn käyttäjille lähettämästä tiedosta sekä ehkä osaa tiedonkäsittelyn ja tietokannan välillä kulkevasta tiedosta. Viimeisenä on *kirjautumisenseuranta*, joka pitää kirjaa siitä, kuka järjestelmään on milloinkin kirjautuneena tai ollut kirjautuneena.

Lohkoketjuilla saataisiin laajimmillaa toteutettua nämä kaikki. Lohkoketjuun tallentuisivat kaikki käyttäjien syötteet. Näitä syötteitä ja valmiiksi tallennettua tietoa käsittelisi lohkoketjuun liitetty älysopimusverkko. Kirjautumisten- ja käytönseuranta tapahtuisi automaattisesti, koska kaikesta toiminnasta jäisi aina aikaleima ja toimijaan liittyvä jälki. Tämän kaltainen toteutus muistuttaisi Ethereumin lohkoketjua (Woods (2014)). Tämä ratkaisu ei olisi kovin hyvä. Suurimpana ongelmana on, että kaikki asiakastiedot olisi tallennettu kuhunkin solmuun. Tämä veisi merkittävän määrän tallennustilaa ja olisi laitonta (L 159/2007, 4 §;L 785/1992, 13 §). Lisäksi on otettava huomioon mahdollisuus, että jotain menee pieleen. Jos käyttäjätietojen salaus onnistuttaisiin jollain keinolla, kuten kvanttilaskennalla, murtamaan, tietova-

ras voisi viedä kaikkien asiakkaiden tiedot mistä vain solmusta.

Voi siis olla järkevää rajoittaa ainakin tietokanta lohkoketjuratkaisun ulkopuolelle. Järkevää voisi olla hoitaa kirjautumisen- ja käytönseuranta lohkoketjun avulla. Ainakin kevyet ja helposti toteutettavat osat tietojenkäsittelystä saataisiin toteutettua älysopimusten avulla. Monimutkaisemmat tietojenkäsittelyn toiminnot, kuten tiedonlouhinta ja tekoälyt kannattanee hoitaa keskitetysti. Tässä ratkaisussa saataisiin hyödynnettyä kaikkia lohkoketjujen ja älysopimuksien hyviä puolia ilman, että vaarannettaisiin asiakkaiden tietoja. Tietokannalle toki tarvittaisiin hyvät varajärjestelmät luotettavuuden takaamiseksi, mutta se on vaatimuksena nykyjärjestelmässäkin. Tämäkään ei ratkaisu ei täytä lain kaikkia vaatimuksia (L 159/2007, 4 §;L 785/1992, 13 §). Tieto edelleen käsiteltäisiin hajautetusti, mikä tarkoittaisi sen tallentamista ainakin hetkellisesti useampaan paikkaan.

Voimme rajata myös tiedonkäsittelyn lohkoketjuratkaisun ulkopuolelle. Tällöin tieto käsiteltäisiin ja tallennettaisiin keskitetysti. Lohkoketju toimisi siis järjestelmän portin vartijana, joka seuraa kuka järjestelmää käyttää ja mitä he sillä tekevät. Tällöinkään ei täysin vältytä asiakastietojen hajauttamiselta, koska tavat, joilla tietoja käytetään tai tallennetaan voidaan käsittää asiakastiedoiksi.

Yksi ratkaisu olisi myös se, että vain kirjautumistiedot tallennetaan lohkoketjuun. Näiden kirjautumistietojen avulla keskitetty tai keskitetynkaltainen käytönseuranta voisi päättää mitä tietoa päästetään varsinaiseen järjestelmään. Tämä saataisiin tehtyä jo lähes lain rajoissa. Ainoana ongelmana on vain vaatimus lokitietojen poistosta (L 159/2007, 5 §). Tähänhän lohkoketju ei pysty.

5.2 Olemassa olevia ratkaisuja

Mettler (2016) tuo esille neljä tapausta, joissa lohkoketju teknologiaa hyödynnetään terveydenhuollon sovelluksissa maailmalla. Nämä ovat Gem Health Network, Healthbank, Accenture Counterfeit Medicine Project ja Guardtime.

Gem Health Network on lohkoketjupohjainen terveydenhuoltoalan kokonaistiedon-

hallinta ratkaisu. Se sisältää tunnistautumistietojenhallinnan, tietokannat ja tiedonkäsittelyn. Gem Health Network toimii Ethereumin älysopimusympäristössä.

Sveitsiläinen start-up-yritys Healthbank on erikoistunut asiakaslähtöisen terveysdatan tallentamiseen lohkoketjujen avulla. Healthbankin liiketoiminta perustuu terveystiedon keräämiseen, varastointiin ja myymiseen sitä tarvitseville.(Mettler (2016))

Accenture Counterfeit Medicine Project keskittyy lääkkeiden alkuperän jäljittämiseen (Mettler (2016)). Lohkoketjuteknologiaa on käytetty jäljittämään myös muiden tuotteiden, kuten kullan ja timanttien alkuperää. Mettler (2016) tuo esille, että Accenture Counterfeit Medicine Project toimii Hyperledger-alustalla. Hyperledger on merkittävä toimija konsortiolohkoketjujen markkinoilla.

Suomen kannalta ehkä merkittävin lohkoketjutoteutus, jonka Mettler (2016) mainitsee, löytyy Virosta. Viron terveydenhuollon tiedot tallentaa yritys nimeltä Guardtime (Mettler (2016)). Huomattavaa on ratkaisun laajuus, jonka Mettler (2016) sanoo olevan "täysivaltainen julkisen terveydenhuollon infrastruktuuri [...] käyttäen lohkoketjua".

6 Yhteenveto

Lohkoketjut ovat aivan uudenlainen teknologia, koska ne mahdollistavat luottamuksettoman, mutta luotettavan, tietojen tallennuksen. Tämän kaltaiselle tietojen tallennukselle on kysyntää terveysalalla, kuten monella muullakin alalla. Suomessa on parhaillaan meneillään merkittävä terveysalan murros, joka osui juuri oikeaan aikaan lohkoketjujen kaltaisen uuden teknologian näkökulmasta.

Lainsäädäntö voi Suomessa rajoittaa lohkoketjujen käyttöä terveydenhuollon sovelluksiin. Osa laeista on hieman vanhanaikaisia, mutta syyt niiden asettamiselle ovat olleet tärkeät. Nämä syyt tulisi huomioida myös mahdollisia uusia ratkaisuja luodessa.

Suomen terveydenhuolto ei vielä sovella lohkoketjuratkaisuja, mutta mielenkiintoa teknologiaan on huomattavissa. Myös lohkoketjupalveluiden tarjoajat ovat kiinnostuneet Suomen terveydenhuollosta mahdollisena asiakkaana.

Tulee olemaan mielenkiintoista nähdä millaisiin ratkaisuihin Suomen terveydenhuollossa päädytään ja tulevatko lohkoketjut olemaan osa niitä. Jos tulevat, on edelleen mielenkiintoista nähdä minkälainen osa.

Kirjallisuutta

Nakamoto, S. 2008. *Bitcoin: A peer-to-peer electronic cash system*. Cryptovest.co.uk.

Woods, G. 2014. *Ethereum: A Secure Decentralized Generalised Transaction Ledger*.

Buterin, V. 2014. *A next generation smart contract & decentralized application platform*.

Bitcoinwikin artikkeli Script-kielestä. Saatavana WWW-muodossa: en.bitcoin.it/wiki/Script. Viitattu 20.5.2017.

Greenspan, G. 2015. *MultiChain Private Blockchain - White Paper*.

Swanson, T. 2015. *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P. 2014. *Enabling Blockchain Innovations with Pegged SideChains*.

Mettler, M. 2016. *Blockchain Technology in Healthcare: The Revolution Starts Here*.

L 159/2007. *Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä*. Viitattu 12.2.2017.

L 785/1992. *Laki potilaan asemasta ja oikeuksista*. Viitattu 12.2.2017.