Opinnäytetyö (AMK)

Tieto- ja viestintätekniikan koulutus

2024

Julius Kuorikoski

Tietoturvan parantaminen lohkoketjuteknologian avulla

– potilastietojärjestelmien suojaaminen

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikan koulutus

Kevät 2024 | 46 sivua

Julius Kuorikoski

Tietoturvan parantaminen lohkoketjuteknologian avulla

- potilastietojärjestelmien suojaaminen

Lohkoketjuteknologialla on tärkeä rooli terveydenhuoltojärjestelmien tiedonhallinnan, turvallisuuden ja yhteentoimivuuden parantamisessa. Tässä opinnäytetyössä tutkittiin lohkoketjun soveltamista potilastietojärjestelmiin ja keskityttiin sen mahdollisuuksiin parantaa potilastietojen saatavuutta, yksityisyyttä ja järjestelmän tehokkuutta.

Lohkoketjupohjaisen potilastietojärjestelmän kehittämisen ja analysoinnin avulla tarkasteltiin keskeisiä näkökohtia, kuten suorituskykyä, turvallisuutta ja säännösten noudattamista. Tutkimuksessa syvennyttiin älysopimusten, salaustekniikoiden ja pääsynvalvontamekanismien suunnitteluun sekä toteuttamiseen, jotta potilastietojen eheys pystytään varmistamaan.

Tutkielmassa käsiteltiin myös skaalautuvuuden tuomia haasteita, ja lohkoketjun käytöstä aiheutuvia kustannuksia. Testisuunnitelman ja turvallisuusanalyysin avulla arvioitiin lohkoketjun integroinnin toteutettavuutta ja tehokkuutta terveydenhuoltojärjestelmissä.

Tutkielma osallistui meneillään olevaan keskusteluun uusien teknologioiden hyödyntämisestä terveydenhuollonjärjestelmien kehittyvien tarpeiden täyttämiseksi.

Asiasanat:

Lohkoketju, tietoturva, potilastietojärjestelmä, älysopimus, Ethereum

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and communications technology

2024 | 46 pages

Julius Kuorikoski

Enhancing data security through blockchain technology

- a focus on securing patient electronic health records

The integration of blockchain technology into healthcare systems has potential to revolutionize data management, security, and interoperability. This thesis examined the application of blockchain to electronic healthcare systems, focusing on its potential to improve access to patient data, privacy, and system efficiency.

Through the development and analysis of a blockchain-based healthcare system, key aspects such as performance, security and compliance were addressed. The study delved into the design and implementation of smart contracts, encryption techniques and access control mechanism to ensure the integrity of patient data.

It also addressed the challenges of scalability and the costs of using blockchain. Through a test plan and security analysis, the study assessed the feasibility and effectiveness of blockchain integration in healthcare systems.

The thesis contributed to the ongoing debate on the use of new technologies to meet the evolving needs of healthcare systems.

Keywords:

Blockchain, data security, electronic healthcare record, smart contract, Ethereum

Sisältö

Kuvat

Taulukot

Käytetyt lyhenteet tai sanasto

2WP	2-Way Peg
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DoS	Denial-of-Service
EHR	Electronic Health Record
ETH	Ether
EU	Euroopan Unioni
EVM	Ethereum Virtual Machine
GDPR	Yleinen tietosuoja-asetus
IoMT	Internet of Medical Things
IPFS	InterPlanetary File System
MitM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPS	Transactions Per Second

1 Johdanto

Teknologisen kehityksen ja digitaalisen muutoksen aikakautena terveydenhuollon tietojen turvallisuus ja eheys ovat nousseet tärkeiksi huolenaiheiksi. Terveydenhuoltojärjestelmiin kohdistuu jatkuvia uhkia liittyen potilastietojen luottamuksellisuuteen, saatavuuteen ja eheyteen, joka edellyttää vankkoja kyberturvallisuustoimenpiteitä arkaluonteisten tietojen suojaamiseksi haitallisilta toimijoilta. Potilastietojen digitalisointi sekä toisiinsa kytkettyjen lääkinnällisten laitteiden ja järjestelmien yleistyminen ovat laajentaneet kyberuhkien hyökkäyspintaa, mikä aiheuttaa merkittäviä riskejä potilaiden yksityisyydelle, ja terveydenhuollon kokonaistehokkuudelle. (Ukyab & Beato, 2024)

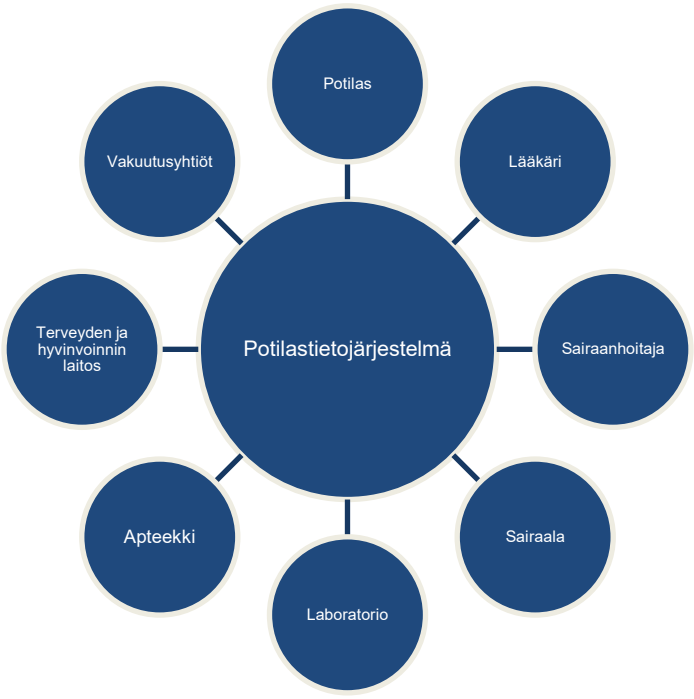
Lohkoketjuteknologian integrointi terveydenhuoltojärjestelmiin on saanut huomiota lupaavana metodina ratkaista kyberturvallisuushaasteita. Alun perin kryptovaluuttoja varten kehitetty teknologia on mukautunut monipuoliseksi työvälineeksi eri toimialoilla. Lohkoketju on muuttumaton ja hajautettu tietokanta, joka varmistaa tietojen eheyden ja turvallisuuden jakamalla ne solmujen verkostoon keskitetyn paikan sijaan. Tämän rakenteen ansiosta lohkoketju soveltuu hyvin terveydenhuoltojärjestelmiin.

Tässä opinnäytetyössä tutkitaan lohkoketjuteknologian soveltamista terveydenhuoltojärjestelmien kyberturvallisuuden parantamiseksi, ja siinä keskitytään erityisesti potilaiden yksityisyyden suojaamiseen ja lääketieteellisten tietojen eheyden varmistamiseen. Hyödyntämällä lohkoketjujen luontaisia ominaisuuksia, kuten hajauttamista, kryptografista turvallisuutta ja väärentämisen estäviä kirjausketjuja, terveydenhuollon organisaatiot voivat vahvistaa puolustustaan kyberuhkia vastaan, ja samalla edistää luottamusta potilaiden keskuudessa.

2 Terveydenhuollon potilastietojärjestelmät

Potilastietojen hallinnassa on kyse potilastietojen käsittelystä ja jakamisesta eri terveydenhuollon toimijoiden sekä potilaan välillä. Sitä varten käytetään erilaisia potilastietojärjestelmiä, joilla pyritään parantamaan terveydenhuollon tietojen tehokkuutta, saatavuutta ja tarkkuutta. Näihin järjestelmiin kuuluvat tyypillisesti sähköiset potilastietojärjestelmät ja pilvipohjaiset terveydenhuoltopalvelut. (Basil ym., 2022)

Suomessa potilastietojärjestelmät ovat jaettu A- ja B-luokkiin. A-luokan järjestelmiä on noin neljänkymmentä ja ne ovat integroitu Kanta-palveluun. A-luokan potilastietojärjestelmät ovat käytössä julkisen terveydenhuollon toimijoilla, ja kaikilla niillä, joilla on käytössään sähköinen resepti tai potilastiedon arkisto. A-luokan järjestelmät edellyttävät ulkopuolista tietoturvallisuuden arviointia. B-luokan potilastietojärjestelmiä on puolestaan noin 260 erilaista, joiden tietoturvallisuuden arviointiin riittää oma ilmoitus. (Lääkärilehti, 2020) Kuva 1 illustroi kaikki eri entiteetit, jotka ovat vuorovaikutuksessa potilastietojärjestelmien kanssa.



Kuva 1. Yleiskatsaus potilastietojärjestelmien saatavuuteen.

Potilaiden terveystietojen arkaluonteisuus korostaa vankkojen turvatoimien merkitystä potilastietojärjestelmissä. Potilastietojen suojaaminen luvattomalta käytöltä, tietoturvaloukkauksilta ja verkkouhilta onnistuu käyttämällä erilaisia turvaprotokollia, salaustekniikoita, pääsynvalvontaa ja todennusmekanismeja. Suomessa Valvira valvoo myös NIS-direktiivin perusteella terveydenhuollon verkko- ja tietoturvallisuutta. (Valvira, n.d.)

Terveydenhuoltoa Suomessa säätelevät terveydenhuoltolaki ja laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007). Terveydenhuoltopalvelujen tarjoajien on säilytettävä potilastietojen luottamuksellisuus ja varmistettava, että arkaluonteisiin tietoihin pääsee käsiksi vain valtuutettu henkilöstö. (Terveydenhuoltolaki 1326/2010) Lisäksi Suomessa on laadittu asiakastietojen sähköistä käsittelyä koskevia ohjeita ja määräyksiä, joilla varmistetaan terveydenhuollon tietojärjestelmien turvallisuus ja yksityisyys. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007)

Yleinen tietosuoja-asetus (GDPR) on Euroopan unionin (EU) kattava tietosuojalaki, jota sovelletaan henkilötietojen käsittelyyn, mukaan lukien sähköiset potilastiedot (EHR). Yleisessä tietosuoja-asetuksessa vahvistetaan periaatteet henkilötietojen lailliselle käsittelylle, mukaan lukien vaatimus saada yksilöiden suostumus heidän terveystietojensa keräämiseen ja käsittelyyn. Yleisen tietosuoja-asetuksen mukaan terveydenhuollon tarjoajien on toteutettava asianmukaisia teknisiä ja järjestöllisiä toimenpiteitä sähköisten potilastietojen turvallisuuden ja luottamuksellisuuden varmistamiseksi. Yksityishenkilöillä on oikeus saada pääsy terveystietoihinsa, pyytää korjauksia, ja tietyissä olosuhteissa vaatia tietojen poistamista. (Euroopan komissio, n.d.)

3 Terveydenhuollon tietojärjestelmien turvaaminen

Tehokas potilashoito vaatii teknologian hyödyntämistä terveydenhuollossa. Tähän liittyy kuitenkin luonnostaan kyberturvallisuusuhkien ja -haavoittuvuuksien riski, jotka asettavat merkittäviä haasteita tietojärjestelmien turvallisuudelle. Tässä luvussa syvennytään potilastietojärjestelmien turvaamiseen, ja tarkastellaan lohkoketjuteknologian mahdollisuuksia näiden haasteiden ratkaisemisessa. Lukijalle selvitetään lohkoketjuteknologian perusteita ja tutkitaan sen hyötyjä terveydenhuollossa.

3.1 Kyberturvallisuusuhat ja -haasteet

- Kiristysohjelmat (Ransomware)

  Haittaohjelmatyyppi, joka estää pääsyn laitteeseen ja siihen tallennettuihin tietoihin. Ensimmäinen ransomware-hyökkäys tapahtui vuonna 1989 ja se kohdistui nimenomaan terveydenhuoltoalalle. (Kruse, C. ym., 2017)

- Tietojenkalastelu (Phishing)

  Phishing on sosiaalisen manipuloinnin muoto, jossa hyökkääjät yrittävät huijata työntekijöitä joko asentamaan haittaohjelmia tai paljastamaan arkaluonteisia potilastietoja. Hyökkäys voi tapahtua esimerkiksi sähköpostiviestin välityksellä, jonka kautta työntekijä avaa epäilyttävän linkin tai tiedoston. (Kruse, C. ym., 2017)

- Väsytyshyökkäys (Brute-force)

  Hyökkääjät voivat käyttää brute force-tekniikkaa saadakseen kirjautumistiedot etäkäyttötyökaluun, jonka kautta uhkatekijä saa itselleen valtuutetun käyttäjän käyttöoikeustason ja pääsee näin sekaantumaan arkaluonteisiin potilastietoihin. (Kruse, C. ym., 2017)

- Sisäpiiriuhka

Sisäpiiriuhka on mahdollisesti terveydenhuollon organisaatiossa työskentelevä henkilö, jolla on sisäpiirin tietoja organisaation turvakäytännöistä ja tietojärjestelmistä. Sisäpiirinuhat voivat toimia tahallisesti tarkoituksena aiheuttaa vahinkoa tai teko voi johtua myös huolimattomuuden ja inhimillisen virheen seurauksena. (U.S. Department of Health and Human Services, 2022)

- Haittaohjelma (Malware)

  Haittaohjelmat ovat ohjelmistoja, joiden tarkoituksena on häiritä, vahingoittaa tai saada luvaton pääsy tietokonejärjestelmiin, verkkoihin tai tietoihin. Noin 40 prosenttia terveydenhuollon haittaohjelmatartunnoista on peräisin pilvisovelluksista. (Alder, S., 2024)

- Tietoturvaloukkaus (Data Breach)

  Tietomurto tarkoittaa arkaluonteisten tietojen luvatonta käyttöä, paljastamista tai varastamista organisaation järjestelmistä. Terveydenhuollon tietomurtojen yleisyys ja laajuus kasvavat nopeasti, joka johtuu internetiin yhdistetyistä laitteista, joista käytetään termiä IoMT (Internet of Medical Things). Hakkeroinnin yhteydessä laitteet voivat paljastaa arkaluonteisia potilastietoja tai aiheuttaa ongelmia hoidon suhteen. (Seh, A. ym. 2020)

- Palvelunestohyökkäys (Denial-of-service, DoS)

  Palvelunestohyökkäys on yritys häiritä verkon tai palvelun normaalia toimintaa tulvimalla siihen liikaa liikennettä tai pyyntöjä. Verkon tietoturvahaasteiden määrä on kasvanut nopeasti langattomien sensoriverkkojen myötä. Siksi pilvipalveluiden infrastruktuurin turvallisuudesta on tullut haaste terveydenhuollon toimijoille. (Mehrtak, M. ym, 2021)

- Man-in-the-Middle (MitM)

Hyökkääjät sieppaavat lääkinnällisten laitteiden, kuten terveysmonitorien tai potilaiden etäseurantajärjestelmien välistä viestintää. Hyökkäyksessä hyödynnetään viestintäprotokollien haavoittuvuuksia tai turvattomia verkkoyhteyksiä. Hyökkääjät voivat peukaloida tai muuttaa potilastietoja ennen kuin ne saavuttavat määränpäänsä. (Salem, O. ym. 2022)

3.2 Tietoturvatavoitteiden määrittely

Terveydenhuollon tietojärjestelmillä on suuri merkitys terveydenhuollon laitoksille, sillä ne mahdollistavat potilastietojen tallentamisen, hakemisen, analysoinnin, vaihdon ja jakamisen. Tietoturvajärjestelmiä käytetään potilaiden yksityisyyden suojan sekä lääketieteellisten tietojen turvallisuuden varmistamiseksi. Potilastietojen luottamuksellisuus, eheys ja saatavuus ovat välttämättömiä laadukkaan terveydenhuollon kriteerejä. (Shojaei, P. ym. 2024)

Seuraavassa osassa käsitellään potilastietojärjestelmien keskeisten turvallisuusvaatimusten periaatteita, määritelmiä ja esimerkkejä.

- Luottamuksellisuus

  Varmistetaan arkaluonteisten potilastietojen olevan saatavilla ainoastaan valtuutetuille tahoille. Tämä saavutetaan valvomalla ja rajoittamalla pääsyä sähköisiin potilastietoihin käyttäjäroolien ja -oikeuksien perusteella.

- Eheys

  Potilastietojen tarkkuuden, johdonmukaisuuden ja luotettavuuden säilyttäminen. Digitaalisia allekirjoituksia käytetään potilastietojen aitouden sekä eheyden todentamiseen.

- Saatavuus

  Varmistetaan potilastietojärjestelmien ja palveluiden toimivan sekä olevan käytettävissä tarpeen vaatiessa. Redundanttien järjestelmien

käyttöönotto ja toipumissuunnitelmien kehittäminen ovat tärkeitä jatkuvuuden varmistamiseksi.

- Todennus

  Käyttäjien ja laitteiden henkilöllisyyden todentaminen potilastietojärjestelmiin pääsyä varten. Terveydenhuollon ammattihenkilöiden tunnistaminen käyttäjätunnuksella ja salasanalla tai sormenjäljellä.

- Valtuutus

  Oikeuksien myöntäminen valtuutetuille käyttäjille roolien ja vastuualueiden perusteella. Määritetään lääkäreille erityiset käyttöoikeudet potilastietojen tarkasteluun erikoistumisen tai osaston perusteella.

- Tarkastettavuus

  Käyttäjien toimintojen ja tapahtumien kirjaaminen ja käyttöoikeuksien seuranta. Kaikkien potilastietoihin kohdistuvien yritysten kirjaaminen, mukaan lukien päivämäärä, kellonaika ja käyttäjän tunnistetiedot, parantaa läpinäkyvyyttä ja helpottaa tarkastusta.

- Salaus

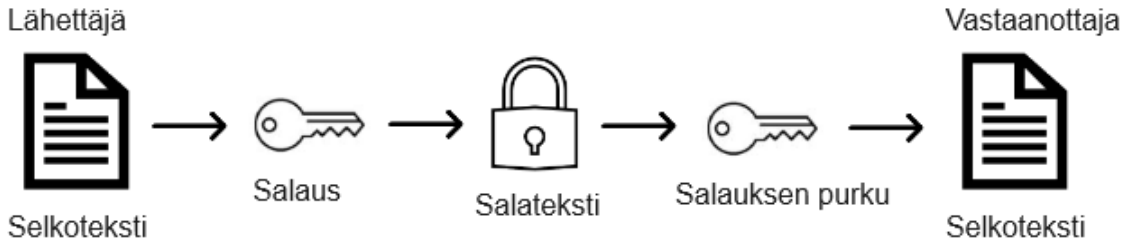
  Suojaa arkaluonteiset potilastiedot salaamalla ne siirron ja tallennuksen aikana. Salaustekniikoita käytetään esimerkiksi terveydenhuoltopalvelujen tarjoajilta apteekeille lähetettävien sähköisten lääkemääräysten suojaamiseksi salakuuntelulta ja luvattomalta käytöltä.

- Vaatimustenmukaisuus

  Potilastietojen turvallisuutta ja yksityisyyttä koskevien lakien, asetusten ja alan standardien noudattaminen. Tämä sisältää kansallisen terveydenhuoltolain sekä lisäksi voidaan vaatia kansainvälisten standardien, kuten ISO/IEC 27001 ja ISO 27799 noudattamista.

3.3 Kryptologia

Kryptografia toimii arkaluonteisten tietojen kilpenä, joka suojaa luvattomalta käytöltä ja ilkivallalta. Ennen kuin syvennytään salaustekniikoihin ja niiden sovelluksiin, luodaan perustiedot keskeisistä termeistä ja käsitteistä. Alkuperäinen viesti, jota kutsutaan **selkotekstiksi**, muunnetaan koodattuun muotoon ja sitä kutsutaan **salatekstiksi**. Tämä prosessi tapahtuu salauksen avulla, kun taas salauksen purkaminen kääntää prosessin päinvastaiseksi ja muuttaa salatekstin takaisin selkotekstiksi. **Kryptografia** eli salausjärjestelmien ja -tekniikoiden tutkimus on tietoturvan kulmakivi, joka kattaa salakirjoitusten suunnittelun, toteutuksen ja analysoinnin. **Salausanalyysi**, eli ”koodin murtaminen”, käsittelee viestien purkamista ilman salausmenetelmien yksityiskohtien tuntemusta. Kryptografia ja salausanalyysi muodostavat yhdessä kryptologian alan, joka on tärkeä arkaluonteisten tietojen suojaamiseksi. Kuvassa 2 on visualisoituna kryptografian eri vaiheet.



Kuva 2. Viestin salaus ja purku

Salausjärjestelmät eroavat toisistaan kolmella keskeisellä tavalla, joista jokainen on tärkeä tietojen salauksen tehokkuuden ja kestävyyden kannalta. (Stallings, W., 2016)

1. Selkotekstin muuntaminen salatekstiksi on keskeinen menetelmä kryptografisissa järjestelmissä. Salausalgoritmeissa hyödynnetään kahta pääperiaatetta. Substituutio, jossa jokainen selkotekstin elementti korvataan toisella ja transponointia, jossa selkotekstin elementit järjestetään uudelleen. Näiden operaatioiden ytimessä on niiden palautettavuus, jolla varmistetaan, ettei tietoa menetetä salauksen

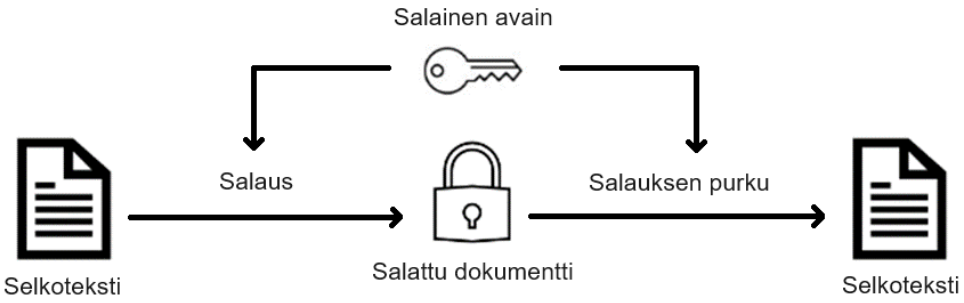
aikana. Monissa salausjärjestelmissä on useita substituutio ja transponointi vaiheita tietoturvan vahvistamiseksi.

2. Käytettävien avainten määrä erottaa toisistaan symmetriset ja epäsymmetriset salausjärjestelmät. Symmetrinen salaus perustuu yhteen ainoaan avaimeen, joka jaetaan lähettäjän ja vastaanottajan kesken turvallista viestintää varten. Epäsymmetrisessä salauksessa käytetään erillisiä avaimia salaukseen ja salauksen purkamiseen, mikä parantaa turvallisuutta, koska vaihtoa ei tarvita.
3. Salausjärjestelmien toiminta riippuu tavasta, jolla selkotekstiä käsitellään. Lohkosalaimet toimivat kiinteillä selkotekstilohkoilla ja ne muodostavat vastaavat salatekstilohkot keskenään, kun taas virtasalaus käsittelee selkotekstin osia jatkuvasti tuottaen tulosteen reaaliaikaisesti.

3.4 Kryptografiset algoritmit

3.4.1 Symmetrinen salaus

Symmetrisiä salausalgoritmeja, kuten Advanced Encryption Standard (AES) ja Data Encryption Standard (DES), käytetään tietojen suojaamiseen salaamalla ja purkamalla tiedot yhdellä jaetulla salaisella avaimella. (Yassein, M. B. ym. 2017) Kuvassa 3 osoitetaan, miten symmetrisessä salauksessa samaa avainta käytetään salaukseen ja sen purkuun.



Kuva 3. Symmetrisen salauksen algoritmi

- AES

AES on lohkosalausalgoritmi, joka käyttää symmetristä avainta sekä salaus- että purkuprosesseihin. National Institute of Standards and Technology (NIST) suosittelee sitä arkaluonteisten tietojen suojaamiseen. AES tukee 128, 192 tai 256 bitin pituisia avaimia, ja se toimii avaimen pituuteen perustuvilla useilla salauskierroksilla.

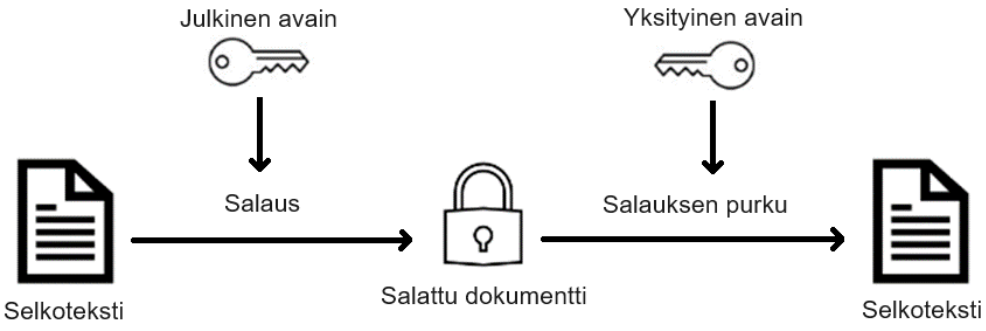
- DES

  DES on yksi varhaisimmista symmetrisistä salausalgoritmeista. Se käyttää 56-bittistä avainta ja toimii 64-bittisillä tietolohkoilla.

Symmetristä salausta käytetään yleisesti viestintäkanavien, kuten sähköpostin, viestisovellusten ja VPN-yhteyksien suojaamiseen. Sitä voidaan myös hyödyntää potilastietojen, tietokantojen tai tallennuslaitteiden salaamiseen tietomurron sattuessa.

3.4.2 Asymmetrinen salaus

Asymmetrinen salaus, joka tunnetaan myös nimellä julkisen avaimen salaus, eroaa symmetrisestä salauksesta niin, että siinä käytetään avainparia – julkista avainta salaukseen, ja yksityistä avainta salauksen purkamiseen. (Yassein, M. B. ym. 2017) Kuvassa 4 nähdään miten salaukseen ja salauksen purkuun käytetään eri avaimia.



Kuva 4. Asymmetrisen salauksen algoritmi

- RSA (Rivest-Shamir-Adleman)

RSA on laajalti käytetty asymmetrinen salausalgoritmi tiedonsiirron ja digitaalisten allekirjoitusten turvaamiseen. Siinä generoidaan julkisen ja yksityisen avaimen pari, jossa julkinen avain jaetaan salausta varten ja yksityinen avain pidetään salassa salauksen purkamista varten

- Diffie-Hellman

  Diffie-Hellman avaintenvaihtoa käytetään salausavainten turvalliseen vaihtamiseen julkisella kanavalla. Sen avulla kaksi osapuolta voi luoda jaetun salaisen avaimen lähettämättä itse avainta.

Asymmetristä salausta käytetään SSL/TLS:n kaltaisissa turvallisissa viestintäprotokollissa, joilla salataan asiakkaiden ja palvelimien välillä internetissä vaihdettavat tiedot. Sitä voidaan hyödyntää myös digitaalisten allekirjoitusten luomiseen sähköisten asiakirjojen tai viestin aitouden ja eheyden todentamiseksi.

3.5 Lohkoketjuteknologia

3.5.1 Lohkoketjujen historiaa

Lohkoketjuteknologia perustuu hajautettuun tietokantaan, jossa jokainen solmu ylläpitää itsenäisesti yksittäisiä tietueita. Lohkoketjuverkon solmut validoivat tapahtumat konsensusalgoritmien avulla. Nämä hajautetut tietokannat varmistavat, että jokainen solmu säilyttää uniikin tietokannan, ja transaktiot todennetaan konsensusmekanismien avulla. Lohkoketjuteknologian muuttumaton luonne tarkoittaa, että kaikki transaktiot tallennettaan hajautettuun tietokantaan, mikä tarjoaa avoimuutta ja turvallisuutta. Lähettäjät sekä vastaanottajat saavat ilmoituksen peukalointiyrityksistä vertaisverkkojen välisten yhteyksien avulla. Tämä varmistaa, että tallennettavat tiedot pysyvät suojattuina. (Tapscott, D. ym. 2016)

Kun lohkoketjuteknologia otettiin ensimmäisen kerran käyttöön rahoitusalalla, sen käyttö laajeni nopeasti mullistaen eri toimialoja, kuten vakuutus-,

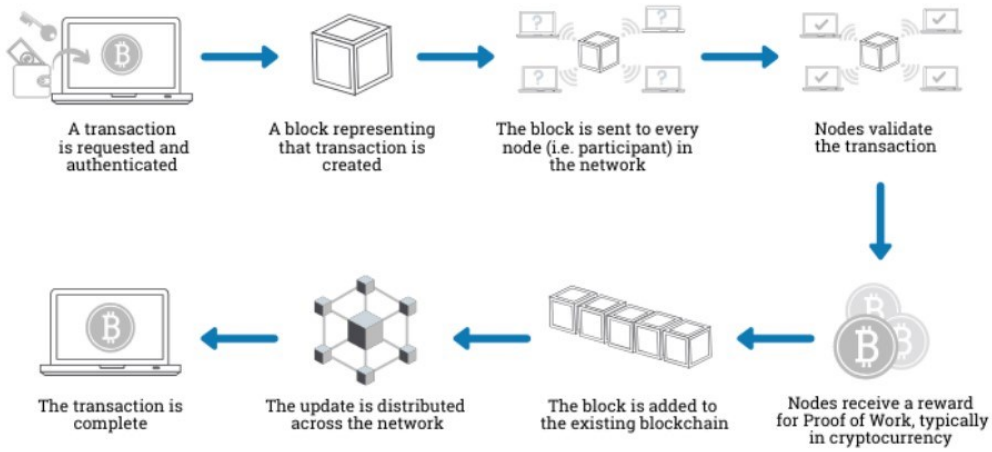
televiestintä-, ilmailu- ja terveydenhuoltoalat. Lohkoketjuteknologian käyttöönoton kehitys voidaan luokitella kolmeen eri vaiheeseen:

1. Lohkoketju 1.0 merkitsi lohkoketjun alkua, kun käyttöön otettiin kryptovaluutta Bitcoin
2. Lohkoketju 2.0 toi ekosysteemiin älykkäät sopimukset, tietueiden seurannan ja omistajuuden todentamisen
3. Tulevaisuutta ajatellen lohkoketjun 3.0 lupaus piilee sen mahdollisuuksissa edistää tieteen ja koulutuksen kehitystä

Lohkoketjuteknologia toimii hajautettuna ja turvallisena järjestelmänä, jossa tapahtumat kirjataan ja todennetaan toisiinsa liitettyjen solmujen verkossa. Sen ensisijaisena tarkoituksena on fasilitoida läpinäkyviä ja väärentämisen kestäviä digitaalisia transaktioita ilman välikäsiä. Lohkoketju suojaa tietoja kryptografisilla tekniikoilla, joilla varmistetaan, että tietokantaan tallennetut tiedot ovat muuttumattomia ja turvattuja. (Tapscott, D. ym. 2016)

Julkisilla ja yksityisillä avaimilla on keskeinen rooli lohkoketjun solmuissa, joissa julkiset avaimet toimivat osoitteina transaktioiden vastaanottamista varten, ja yksityisiä avaimia käytetään kryptografisiin allekirjoituksiin transaktioiden valtuuttamiseksi. Lohkoketjuverkon solmut ovat yhteydessä toisiinsa vertaisverkon kautta, mikä mahdollistaa suoran viestinnän ja tietojen jakamisen osallistujien kesken. (Tapscott, D. ym. 2016)

Lohkoketju käsittelee ulkoisen tiedon tallentamista oraakkelien avulla. Oraakkelit ovat luotettavia lähteitä, jotka toimittavat ulkoista tietoa lohkoketjuun älykkäiden sopimusten suorittamista varten. Lohkoketjuverkon louhijoilla on ratkaiseva rooli transaktioiden validoinnissa, verkon suojaamisessa ja uusien lohkojen lisäämisessä lohkoketjuun. Uusi lohko luodaan lohkoketjuverkkoon konsensusmekanismilla, jossa louhijat kilpailevat monimutkaisten matemaattisten arvoitusten ratkaisemisesta transaktioiden validoimiseksi ja uuden lohkon liittämiseksi olemassa olevaan ketjuun. (Tapscott, D. ym. 2016) Alla olevassa kuvassa 5 nähdään lohkoketjun toiminnallisuudet ja sen eri vaiheet.



Kuva 5. Yleiskatsaus lohkoketjun toiminnallisuudesta (U.S. Department of Health and Human Services, 2021)

Lohkoketjuteknologialla on keskeinen rooli välikäsien poistamisessa ja ketjupohjaisten transaktioiden fasilitoinnissa. Lohkoketjun toisiinsa liitetyt lohkot takaavat jatkuvan ja turvatun tallenteen transaktioista. Kun käyttäjät ovat sopineet transaktiosta, se todennetaan käyttäjien antamien kryptografisten avainten avulla. Kullakin käyttäjällä on yksityinen avain tapahtuman allekirjoittamista varten, ja julkinen avain tarkistamista varten. Transaktiotiedot sisältävä lohko lähetetään verkon jokaiseen solmuun validointia varten. Solmut käyttävät Proof of Work (PoW) -menetelmää tapahtumien todentamiseen, mikä suojaa verkkoa mahdollisilta hyökkäyksiltä. Solmut saavat PoW-prosessin onnistuneesta suorittamisesta kryptovaluuttapalkkion. Kun validoitu transaktio lisätään lohkoketjuun, tiedot leviävät verkossa P2P-mekanismin (Peer-to-Peer) avulla. Suoritettu transaktio tarkoittaa turvallista ja todennettua merkintää lohkoketjun tietokannassa. (U.S. Department of Health and Human Services, 2021)

3.5.2 Kryptovaluutat

Kryptovaluutat ovat lohkoketjuteknologiaa hyödyntäviä sovelluksia, jotka ovat suunniteltu toimimaan turvallisena vaihtovälineenä. Kryptovaluutat toimivat

lohkoketjujen hajautetuissa verkoissa, jotka takaavat avoimuuden ja turvallisen vaihdon. Toisin kuin perinteisiä valuuttoja, kryptovaluuttoja ei valvo keskusviranomainen, kuten hallitus tai pankki. Sen sijaan ne luottavat tietokoneiden vertaisverkkoon, joka validoi ja tallentaa transaktiot. (Härdle, W. ym. 2020)

Bitcoin oli ensimmäinen kryptovaluutta, joka otettiin käyttöön vuonna 2008, ja sen jälkeen on syntynyt lukuisia muita kryptovaluuttoja. Hinnan epävakaus, kyberhyökkäykset ja skaalausongelmat aiheuttavat huolia Bitcoinista maksuvälineenä, mutta teknologiainnovaationa sen hyötyjä ei kannata laiminlyödä. (Berentsen, A. ym. 2018)

3.5.3 Lohkoketjun komponentit

- Desentralisaatio

  Desentralisaatio tarkoittaa lohkoketjussa hallinnan ja päätöksenteon siirtämistä yksilöltä hajautettuun verkkoon. Hajautetut verkot pyrkivät vähentämään yksilön tarvetta osoittaa luottamusta kolmansille osapuolille.

- Lohkoketjualusta

  Lohkoketjualusta on digitaalinen infrastruktuuri, joka mahdollistaa lohkoketjuverkkojen luonnin ja toiminnan. Se tarjoaa tarvittavat työkalut, protokollat ja toiminnallisuudet hajautettujen sovellusten (DApps) rakentamiseen ja käyttöönottoon lohkoketjussa. Esimerkiksi Ethereum tunnetaan älykkäiden sopimusten tuesta ja hajautettujen sovellusten kehittämisestä.

- Konsensusmekanismi

  Konsensusmekanismi on joukko vaiheita, joita lohkoketjuverkon solmut noudattavat sopiakseen ehdotetusta tilasta tai arvosta.

Konsensusmekanismeja tarvitaan säilyttääkseen lohkoketjuverkon eheys ja päästäkseen yhteiseen sopimukseen.

- Älysopimus

  Älysopimus on desentralisoitu applikaatio, joka edustaa osapuolten välistä sopimusta. Se on ohjelmointikielellä kirjoitettu koodi, joka sisältää toimintalogiikan ja se tulee automaattisesti täytäntöön sopimuksen varmistuksen jälkeen.

- Tokenisaatio

  Digitaalisen omaisuuden tokenisointi on prosessi, jossa omaisuuden omistusoikeudet esitetään digitaalisina tokeneina ja ne tallennetaan lohkoketjuun. Ne voivat edustaa lähes mitä tahansa arvoesinettä, mukaan lukien fyysiset, digitaaliset, korvattavissa olevat ja ei-korvattavissa olevat omaisuudet.

- Yhteensopivuus ja skaalautuvuus

  Lohkoketjuteknologian haasteisiin kuuluu niiden yhteensopivuus ja skaalautuvuus. Yhteensopivuudella tarkoitetaan eri alustojen kykyä kommunikoida keskenään. Tällä hetkellä monet lohkoketjuverkot toimivat itsenäisesti. Skaalautuvuudella tarkoitetaan lohkoketjuverkon kykyä käsitellä suuria määriä transaktioita ja käyttäjiä ilman sen hidastumista.

- Louhinta

  Louhintaprosessissa lohkoketjuun lisätään uusia lohkoja. Lohkot sisältävät transaktioita, jotka verkon louhintasolmut validoivat louhintaprosessin avulla. Kun lohkot ovat louhittu ja vahvistettu, ne lisätään lohkoketjuun. Louhinta käyttää paljon resursseja, kuten laskentatehoa ja sähköä.

3.5.4 Lohkoketjutyypit

Julkinen lohkoketju:

Julkisessa lohkoketjussa kaikki tapahtumat ovat julkisesti nähtävillä ja jossa kuka tahansa voi osallistua konsensusprosessiin. Transaktiot validoidaan solmujen hajautetussa verkossa eri konsensusmekanismeilla, kuten PoW ja PoS (Proof of Stake). Verkoston hajautetun luonteen vuoksi julkiseen lohkoketjuun kirjattuja tapahtumia on lähes mahdotonta väärentää. Kun transaktio on lisätty lohkoon ja verkko on vahvistanut sen, siitä tulee osa pysyvää ja muuttumatonta tietuetta. Julkiset lohkoketjut ovat kasvattaneet suosiotaan avoimuuden, läpinäkyvyyden ja turvallisuusominaisuuksien ansiosta. Niitä käytetään yleisesti Bitcoinin ja Ethereumin kaltaisissa kryptovaluutoissa, joissa koko transaktiohistoria on julkisesti saatavilla. (Zheng, Z. ym. 2017)

Yksityinen lohkoketju:

Yksityisessä lohkoketjujärjestelmässä verkkoon pääsy ja osallistuminen konsensusprosessiin on rajoitettu tiettyyn ryhmään tai organisaatioon. Toisin kuin julkiset lohkoketjut, jotka ovat avoimia, yksityiset lohkoketjut ovat täysin yhden tahon tai organisaation hallinnassa, joka tekee niistä keskitettyjä luonteeltaan. Tämä antaa organisaatiolle täydet valtuudet verkkoon, mukaan lukien kyvyn määrittää konsensusmekanismit ja käyttöoikeudet. Osallistuminen yksityiseen lohkoketjuverkkoon on rajoitettu solmuihin, jotka valvova organisaatio on ennalta hyväksynyt. Pääsy transaktiotietoihin voidaan rajoittaa valikoidulle osallistujille. Yksityisiä lohkoketjuja käytetään usein yritysympäristöissä, joissa yksityisyys, valvonta ja skaalautuvuus ovat tärkeitä. Ne tarjoavat yritykselle turvallisen ja tehokkaan tavan hallita ja jakaa tietoja suljetussa ekosysteemissä. (Zheng, Z. ym. 2017)

Konsortio lohkoketju:

Konsortio lohkoketjut ovat julkisen ja yksityisen lohkoketjun yhdistelmä, joka on osittain hajautettu. Siellä on joitakin valvovia solmuja, jotka tarkistavat ja

validoivat transaktioita tai lohkoja. Louhintalohkot ovat voimassa vain, kun kontrolloivat solmut ovat hyväksyneet ja allekirjoittaneet ne. Konsortio lohkoketjujen ongelmana on niiden yhteentoimivuus. (Haque, A. K. M. B. ym. 2023)

Sivuketju:

Sivuketju on toissijainen lohkoketju, joka toimii rinnakkain ensisijaisen lohkoketjun eli pääketjun kanssa. Se mahdollistaa varojen tai tietojen siirtämisen päälohkoketjusta sivulohkoketjuun ja päinvastoin. Sivuketjuja käytetään usein uusien ominaisuuksien toteuttamiseen, skaalautuvuuden parantamiseen tai toimintojen mukauttamiseen vaikuttamatta suoraan pääketjun toimintaan. Esimerkiksi Bitcoin lohkoketjussa ottaakseen käyttöön älysopimukset tai tukeakseen nopeampia transaktioita, kehittäjät voivat luoda sivuketjun, joka tunnetaan nimellä ”Bitcoin Smart Contract Sidechain”. Tämä sivuketju toimii itsenäisesti, mutta on edelleen yhteentoimiva pääketjun kanssa. Käyttäjät voivat siirtää bitcoineja pääketjusta sivuketjuun käyttämällä kaksisuuntaista peg-mekanismia (2WP), jossa bitcoinit lukitaan pääketjussa, kun taas vastaavat tokenit luodaan sivuketjuun. Näitä tokeneita voidaan käyttää sivuketjussa älykkäiden sopimusten toteuttamiseen tai nopeampien transaktioiden suorittamiseen. (Singh, A. ym. 2020)

Taulukko 1. Lohkoketjualustojen ominaisuudet

Teknologia	Konsensus	Performanssi (TPS)	Älysopimus	Sivuketju	DApps
Ethereum	PoS	15-30	Kyllä	Kyllä	Kyllä
Hyperledger Fabric	PBFT	1000-2000	Kyllä	Ei	Kyllä
Quorum	RAFT	1000-2000	Kyllä	Kyllä	Kyllä
Bitcoin	PoW	3-7	Ei	Ei	Ei
Solana	PoH	65 000	Kyllä	Kyllä	Kyllä
Polygon	PoS	7500	Kyllä	Kyllä	Kyllä

3.6 Ethereum: Lohkoketjualustan toiminnallisuus

Ethereum on ympäri maailmaa sijaitsevien tietokoneiden verkosto, jotka noudattavat Ethereum protokollan sääntöjä. Ethereumin kaltaiset julkiset lohkoketjut mahdollistavat kenen tahansa pystyvän lisäämään, mutta ei poistamaan tietoja lohkoketjusta. Tämä tekee hajautetuista lohkoketjuista turvallisia. Ethereumilla on oma kryptovaluutta, Ether (ETH), jolla maksetaan tietyistä verkon toiminnoista. Sitä voidaan siirtää verkon toisille käyttäjille tai vaihtaa muihin Ethereumissa oleviin tokeneihin. ETH:lla maksetaan laskentatehosta, jota tarvitaan sovellusten rakentamiseen ja pyörittämiseen. Ethereumilla on rakennettu yli 4000 projektia, tehty 53,3 miljoonaa älysopimusta ja 96 miljoonaa käyttäjää omistaa Etheriä, joilla tehdään 1,272 miljoonaa päivittäistä transaktiota. (Ethereum, n.d.)

Ethereum Virtual Machine (EVM) on Ethereum-verkon keskeinen osa, joka huolehtii älysopimusten käyttöönotosta ja toteuttamisesta. EVM asettaa älykkäiden sopimusten suorituksille kaasurajoituksia väärinkäytösten estämiseksi. Kaasu on yksikkö, jota käytetään mittaamaan laskennallista tehoa, joka vaaditaan operaatioiden suorittamiseen Ethereum verkossa (Antonopoulos, A. M. ym. 2018)

3.6.1 Ethereum älysopimukset

Älysopimukset ovat Ethereumin lohkoketjuun tallennettuja tietokoneohjelmia, jotka määrittelevät ja panevat täytäntöön koodiin kirjoitetut osapuolten väliset sopimukset. Ne poistavat välikäsien tarpeen suorittamalla sopimuksen automaattisesti ennalta määriteltyjen ehtojen perusteella. (Ethereum, n.d.) Älysopimukset kirjoitetaan yleensä korkean tason kielellä, kuten Solidityllä. Niiden suorittaminen vaatii kuitenkin, että ne käännetään matalan tason byte-koodiksi, joka toimii EVM:ssä. Älysopimusten avainpiirteitä:

1. Toiminnallisuus: Älysopimukset voivat pitää hallussaan ja siirtää tokeneita, hallita oikeuksia, suorittaa logiikkaan perustuvia syötteitä ja

olla vuorovaikutuksessa muiden sopimusten kanssa. Ne ovat muuttumattomia käyttöönoton jälkeen ja näin ollen tarjoavat läpinäkyvyyttä ja luottamusta koodin suorittamiseen.

2. Token-standardit: Ethereum tukee erilaisia token-standardeja, kuten ERC-20 (fungible tokenit) ja ERC-721 (non-fungible tokenit). Nämä standardit määrittelevät yhteiset rajapinnat tokeneita varten, mikä mahdollistaa yhteensopivuuden eri sovelluksissa.
3. Turvallisuusnäkökulmat: Älysopimusten kehittäminen edellyttää parhaiden käytäntöjen noudattamista, kuten syötteen validointia, pääsynvalvontaa ja suojautumista yleisiltä haavoittuvuuksilta, esim. reentracy-hyökkäyksiltä. Tarkastukset, testaukset ja yhteisön standardien noudattaminen ovat tärkeitä turvallisten sopimusten kehittämisessä. (Ethereum, n.d.)

3.6.2 Ethereum DApps

DApp on sovellus, joka toimii keskitetyn palvelimen sijaan hajautetussa tietoverkossa (lohkoketjussa). Seuraavassa osassa selitys mitä ne ovat ja miten ne toimivat:

- Arkkitehtuuri

  DAppsit koostuvat tyypillisesti älysopimuksista, jotka ovat sijoitettu lohkoketjuun ja ne käsittelevät liiketoimintalogiikkaa ja tietojen tallennusta. Frontend -käyttöliittymä on vuorovaikutuksessa älysopimusten kanssa web-käyttöliittymien tai muiden asiakasohjelmien kautta.

- Hajautettu luonne

  DAppsit hyödyntävät lohkoketjuteknologian hajautettua luonnetta yksittäisten vikojen poistamiseksi, ja ne vähentävät tarvetta käyttää kolmansia osapuolia. DAppsit toimivat itsenäisesti älysopimuksiin koodattujen ennalta määriteltyjen sääntöjen perusteella.

- Ominaispiirteet

  DAppseilla on hyvä resilienssi, sillä ne ovat hajautettu useisiin solmuihin lohkoketjuverkossa, joka auttaa niitä kestämään käyttökatkoksia ja sensuuria. Lohkoketjuteknologian läpinäkyvä luonne antaa käyttäjille mahdollisuuden verifioida sovelluksen koodin ja edistää luottamusta. DAppsit hyötyvät lohkoketjuteknologian turvallisuusominaisuuksista, kuten kryptografisesta salauksesta ja konsensusmekanismeista, jotka varmistavat tietojen eheyden ja suojaavat niitä peukaloinnilta. (Ethereum, n.d.)

3.6.3 Ethereumin konsensusmekanismit

Konsensusmekanismeilla varmistetaan, että hajautetut solmut ovat yksimielisiä lohkoketjun tilasta. Ne kattavat laajan joukon ideoita, protokollia ja kannustimia (mm. PoS ja PoW), joilla pyritään suojautumaan Sybil-hyökkäyksiltä ja säilyttämään verkon eheys. Ethereumin yhteydessä konsensus saavutetaan, kun vähintään 66 prosenttia solmuista on yhteysymmärryksessä lohkoketjun statuksesta. (Ethereum, n.d.)

1. Proof of Work: Alun perin Ethereum käytti PoW-menetelmää, jossa louhijat kilpailevat monimutkaisten matemaattisten yhtälöiden ratkaisemisesta uusien lohkojen luomiseksi. Verkon turvallisuus perustuu laskentatehoon, joten hyökkääjien on taloudellisesti mahdotonta manipuloida lohkoketjua.
2. Proof of Stake: PoS on konsensusmekanismi, jota käytetään lohkoketjuverkoissa transaktioiden varmistamiseen ja uusien lohkojen luomiseen. PoS-järjestelmässä validoijat valitaan luomaan uusia lohkoja ja validoimaan transaktioita sen Etherin määrän perusteella, joka heillä on hallussaan ja jonka he ovat valmiita ”stakeemaan” eli panostamaan vakuudeksi. PoS turvaa verkon tekemällä ilkivaltaisen toiminnan taloudellisesti kannattomaksi. PoS on energiatehokkaampi kuin PoW, sillä validoijien ei tarvitse suorittaa intensiivisiä laskutoimituksia. Validoijat

palkitaan osallistumisesta lohkojen luomiseen ja transaktioiden validointiin, joka kannustaa aktiivisuuteen.

3.7 Lohkoketjuteknologian käyttö terveydenhuollossa

Korkeat ylläpito- ja hallintokustannukset kuuluvat nykyisen terveydenhuoltojärjestelmän haasteisiin. Potilastietojen hallinta on työlästä ja sitä vaikeuttaa erilaiset tietorakenteet, järjestelmät ja työnkulut terveydenhuollon eri osa-alueilla. (Ghosh, P. ym. 2023) Perinteisistä kolmannen osapuolen potilastietojärjestelmistä puuttuu läpinäkyvyys. Lohkoketjuteknologia tarjoaa mahdollisuuksia ratkaista nämä yleiset ongelmat. Tietojen eheys saadaan luomalla läpinäkyvä ja muuttumaton tallenne kaikista tapahtumista. Tämä auttaa ylläpitämään potilastietojen, hoitosuunnitelmien ja muiden kriittisten tietojen tarkkuutta ja johdonmukaisuutta. Lohkoketju helpottaa saumatonta tiedonvaihtoa ja yhteensopivuutta eri terveydenhuoltojärjestelmien välillä. Se mahdollistaa potilastietojen turvallisen jakamisen eri alustoilla säilyttäen tietojen yksityisyyden. Virtaviivaistamalla organisaation hallinnollisia prosesseja ja poistamalla välikäsiä voidaan parantaa toiminnan tehokkuutta ja vähentää kustannuksia. Älysopimukset voivat automatisoida tehtäviä, kuten korvausvaatimusten käsittelyä ja maksuja. (Haleem, A. ym. 2021)

3.7.1 Keskeiset näkökohdat lohkoketjuille terveydenhuollossa

Turvallisuus ja yksityisyys:

- Turvallisuus: Terveydenhuoltojärjestelmät tarvitsevat tehostettuja turvatoimia potilastietojen suojaamiseksi luvattomalta käytöltä. Lohkoketjuteknologia tarjoaa salaustekniikoita ja hajautettua tallennusta lääketieteellisten tietojen eheyden ja aitouden varmistamiseksi.
- Yksityisyys: Lohkoketju mahdollistaa potilastietojen turvallisen jakamisen ja se suojaa samalla tietojen yksityisyyttä. Ainoastaan asiankuuluvat sidosryhmät voivat tarkastella ja olla vuorovaikutuksessa niiden kanssa.

Pääsynvalvonta ja todennus:

- Pääsynvalvonta: Potilaat voivat valvoa kuka pääsee käsiksi heidän terveystietoihinsa ja myös myöntää tai peruuttaa pääsyn tietyiltä tahoilta.
- Todennus: Vankoilla todennusmekanismeilla terveydenhuollon tietoja käyttävien käyttäjien henkilöllisyys voidaan todentaa, joka vähentää luvattoman käytön riskiä.

Tietojen muuttumattomuus ja eheys:

- Muuttumattomuus: Lohkoketjuun tallennettuja tietoja ei voi muuttaa tai peukaloida, eli terveydenhuollon tarjoajat ja potilaat voivat luottaa siihen, että tiedot pysyvät väärentämättöminä.
- Eheys: Kaikki tietoihin tehdyt muutokset tai päivitykset kirjataan ja ne voidaan jäljittää niiden lähteeseen, mikä varmistaa tietojen tarkkuuden ja luotettavuuden.

Saatavuus:

- Saatavuus: Käyttämällä hajautettua verkkoa voidaan vähentää tietojen katoamisen tai järjestelmävikojen riskiä, ja varmistaa, että tiedot ovat saatavilla silloin, kun niitä tarvitaan.

Tietojen pätevyys:

- Pätevyys: Käyttämällä konsensusalgoritmeja voidaan varmistaa, että lohkoketjuun lisätään vain päteviä ja todennettuja tietoja.

Skaalautuvuus ja yhteensopivuus:

- Skaalautuvuus: Terveydenhuollon yhteydessä skaalautuvuus on ratkaisevan tärkeää, jotta lohkoketju pystyy käsittelemään järjestelmien suuren transaktio- ja tietomäärän ilman, että sen suorituskyky kärsii.
- Yhteensopivuus: Yhteensopivuudella tarkoitetaan eri lohkoketjuverkkojen kykyä kommunikoida ja vaihtaa tietoja saumattomasti. Potilastietoja voidaan jakaa eri terveydenhuollon tarjoajien ja järjestelmien välillä. (Namasudra, S. ym. 2021)

3.7.2 Lohkoketjun hyödylliset sovellukset terveydenhuollossa

Sähköiset potilastiedot:

- Terveydenhuollossa syntyy huomattavia määriä erilaisia potilastietoja, kuten esimerkiksi terveysarvioita ja hyvinvointikyselyjä. Terveydenhuollon palveluntarjoajat selaavat säännöllisesti tätä valtavaa tietomäärää ja kyseenalaistavat sen tarkkuuden. Lohkoketjuteknologia tarjoaa saumattoman ratkaisun näiden tietojen aitouden todentamiseen vertaamalla niitä lohkoketjujärjestelmässä oleviin tietueisiin. Potilaskohtaamisten aikana sähköiseen potilastietojärjestelmään dokumentoidaan yleensä tärkeät tiedot, kuten potilaan nimi, syntymäaika, diagnoosi, hoidot ja sairaushistoria. Tyypillisesti nämä tiedot tallennetaan pilvipalveluihin tai perinteisiin tietokantoihin. Monissa tapauksissa sähköiset terveystietokannat ovat hajallaan useissa eri terveydenhuollon laitoksissa, mikä johtaa pirstaleiseen tiedonsaantiin ja epäyhtenäiseen potilashoitoon. Lohkoketjuteknologian avulla nämä hajanaiset tiedot voidaan yhtenäistää. (Namasudra, S. ym. 2021)

Vaikutusten analysointi:

- Tutkijat voivat hyödyntää minkä tahansa toimenpiteen vaikutusta suuressa osassa potilaspopulaatiota, kun he saavat potilastiedot käyttöönsä. Esimerkiksi apteekit pystyvät opastamaan potilaita tehokkaammin, miten mukautettuja reseptilääkkeitä tai palveluja tulee käyttää näiden tulosten perusteella. (Namasudra, S. ym. 2021)

Diagnosointi:

- Sujuva tiedonvaihto lääketieteellisten ratkaisujen tarjoajien välillä voi edistää diagnostiikan tarkkuutta, tehokkaita hoitoja ja kustannustehokkaita ekosysteemejä terveydenhuoltojärjestelmässä. (Namasudra, S. ym. 2021)

Kliininen tutkimus:

- Lohkoketjuteknologiaa käytetään kliinisissä tutkimuksissa ratkaisemaan väärien tulosten aiheuttamia epätarkkuuksia, jotka eivät vastaa tutkimuksen tarkoitusta ja tavoitteita. Lohkoketju vahvistaa luottamusta kliinisiin tutkimuksiin. (Namasudra, S. ym. 2021)

Tiedon esittäminen:

- Lohkoketjulla pystytään todistamaan tiedot lääkkeen alkuperästä, jotta voidaan varmistaa lääkkeen korkea laatu ja se, että hyväksytyn lääkkeen valmistaja toimittaa sen. (Namasudra, S. ym. 2021)

Turhien kulujen eliminointi:

- Eliminoimalla tarvetta kolmansille osapuolille, voidaan vähentää turhia yleiskustannuksia. Lohkoketjuteknologialla pystytään ratkaisemaan monet terveydenhuoltojärjestelmää vaivaavat ongelmat, kuten yhteensopivuus, raporttien täydentäminen, varkaudet tai katastrofien aiheuttamat tietomurrot. (Namasudra, S. ym. 2021)

Turvallisuuden parantaminen:

- Validoimalla ja jäljittämällä lääkkeet voidaan lisätä yleistä turvallisuutta potilaiden hoidossa. Sillä estetään esimerkiksi väärennöksien joutumista markkinoille. Lohkoketjut mahdollistavat kaiken tiedon tallentamisen keskitettyyn paikkaan, jolloin potilastietojen tarkasteleminen on helpompaa, ja lääkärit pystyvät tekemään nopeampia ja tarkempia diagnooseja. (Namasudra, S. ym. 2021)

Tietojen muuttaminen:

- Lohkoketjuverkojen avulla voidaan minimoida kustannusten määrää ja tietojen muuttamiseen kuluvaa aikaa. Ne takaavat potilaiden anonymiteetin ja suojan. Lohkoketjun implementointi mahdollistaa tapahtumahistorian ja dokumentoinnin tallentamisen aikaleimalla. Verkon jokainen solmu tarkistaa ja tallentaa jokaisen syötetyn tiedon pätevyyden. (Namasudra, S. ym. 2021)

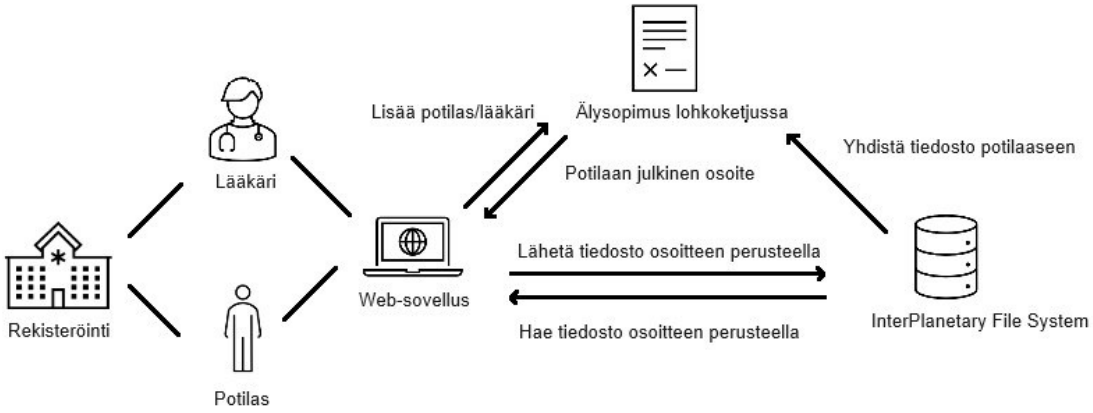
4 Lohkoketjupohjaisen potilastietojärjestelmän suunnittelu ja toteutus

4.1 Järjestelmämalli

Potilastietojärjestelmä koostuu kolmesta pääkomponentista;

1. React web-käyttöliittymä
2. Solidity älysopimus Ethereum lohkoketjussa
3. InterPlanetary File System (IPFS)

Ehdotetussa järjestelmässä potilaiden potilastiedot tallennetaan IPFS nimiseen hajautettuun tiedostojärjestelmään. Terveydenhuollon tarjoaja pystyy rekisteröimään itsensä ja potilaan kryptolompakon julkisella osoitteella. Kun potilaalle on luotu digitaalinen identiteetti, lääkäri voi ladata järjestelmään uuden tallenteen potilastiedoista ja yhdistämään sen kyseiseen identiteettiin. Potilas pääsee tarkastelemaan tietojaan kirjautumalla web-käyttöliittymään ja vuorovaikuttamalla Ethereumin lohkoketjussa olevan älysopimuksen kanssa. Kuva 6 havainnollistaa järjestelmämallin entiteetit ja niiden operaatiot.



Kuva 6. Järjestelmämalli

Potilastietojärjestelmäsuunnitelmaan kuuluvat entiteetit;

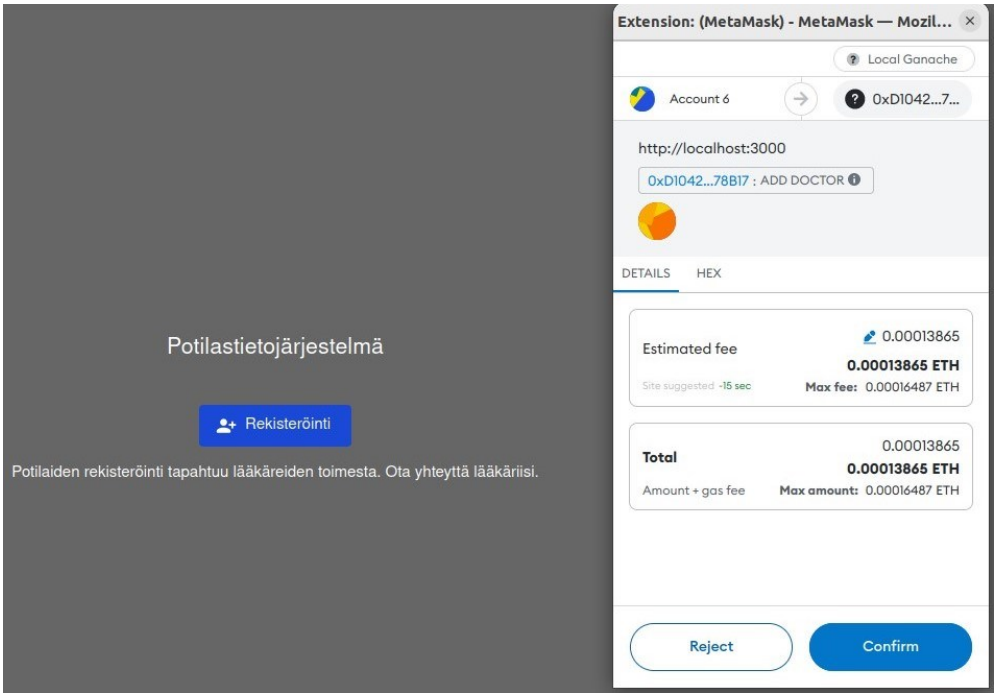
1. Rekisteröintipiste

2. Lääkäri
3. Potilas
4. Web-sovellus
5. Älysopimus Ethereumin lohkoketjussa
6. IPFS

4.2 Skenaario

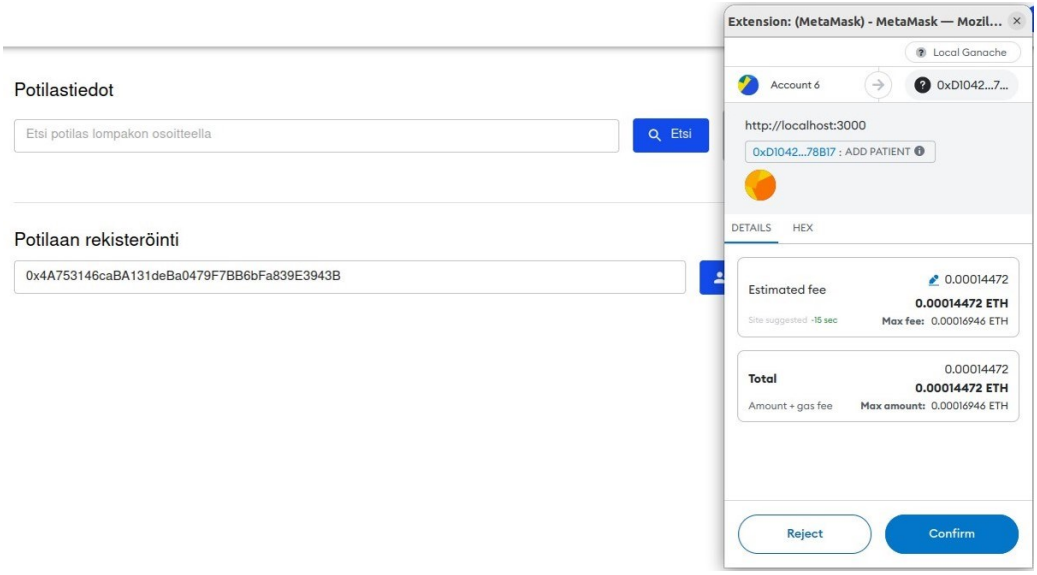
Seuraavaksi käydään läpi havainnollistava mallitapaus.

1. Saadakseen kryptolompakon julkisen osoitteen ja digitaalisen identiteetin, potilaan tulee käydä ennen ensimmäistä ajanvarausta rekisteröintipisteellä, jossa hänen henkilöllisyytensä tarkastetaan.
2. Kuvassa 7 nähdään miten terveydenhuollon tarjoaja, eli tässä tapauksessa lääkäri, voi rekisteröityä järjestelmään käyttämällä kryptolompakkoa, kuten Metamask.



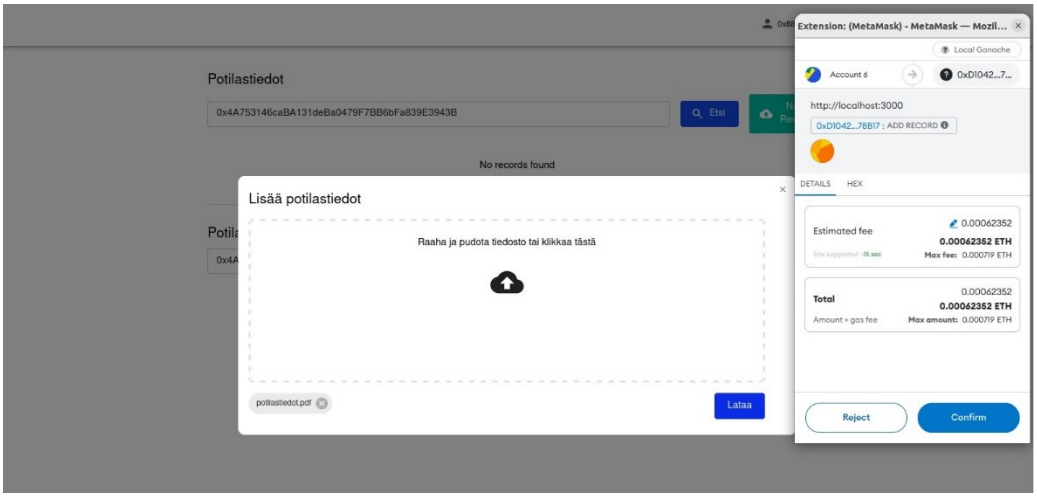
Kuva 7. Lääkärin rekisteröinti potilastietojärjestelmään

3. Potilaan rekisteröinti tapahtuu lääkärin toimesta käyttämällä potilaan saamaa julkista osoitetta, joka annettiin ajanvarauksen yhteydessä. Kuvassa 8 lääkäri rekisteröi potilaan.



Kuva 8. Potilaan rekisteröinti lääkärin toimesta

4. Lääkäri voi selata potilaan tietoja julkisella osoitteella ja ladata uudet tai muokatut potilastiedot järjestelmään kuvan 9 mukaisesti.



Kuva 9. Potilastietojen lisääminen

5. Kuvassa 10 nähdään, miten potilas pystyy kirjautumaan web-käyttöliittymään ja lukemaan sitä kautta omia potilastietoja.

Kuva 10. Potilastietojen tarkastelu

5 Simulaatio ja analyysi

5.1 Ethereum simulaatio

Tässä osassa käydään läpi ehdotetun potilastietojärjestelmän simulaatiota. Suunniteltu järjestelmä ja älysopimus toimii Ethereumin lohkoketjussa. Simulaatiossa käytettiin henkilökohtaista Ethereum lohkoketjua nimeltä Ganache. Ethereumin käyttäjät maksavat kaasumaksuja, eli transaktiomaksuja, transaktioiden suorittamisesta. Näihin lukeutuu esimerkiksi ETH:n lähettäminen, vaihtaminen ja älysopimusten suorittaminen.

5.1.1 Stakeeminen

Ethereumin stakeemisessa validoijat lukitsevat tietyn määrän Etheriä vakuudeksi osallistuakseen verkon PoS-konsensusmekanismiin. Validoijat ovat vastuussa Ethereumin lohkoketjun transaktiolohkojen ehdottamisesta ja validoinnista. Vastineeksi palveluistaan validoijat saavat Etheriä palkkioksi. Etherin määrä muodostuu lohkopalkkioista sekä transaktiokustannuksista, joista validoijat saavat pienen osan.

5.1.2 Kaasu ja transaktiokustannukset

Ethereumissa kaasu on yksikkö, jolla mitataan transaktion suorittamiseen vaadittavaa laskennallista vaivaa. Mitä monimutkaisempi transaktio, sitä suuremmat kulut. Ethereum-verkossa tapahtuvaan transaktioon kuuluu perusmaksu, joka poltetaan ja prioriteettimaksu, joka maksetaan verkon validoijille. Molempiin maksuihin vaikuttaa markkinavoimat eli maksun hinta nousee verkon ruuhkautuessa. Taulukossa 3 nähdään operaatioihin käytetyn kaasun määrä ja sen hinta euroissa. Keskimääräinen kaasun hinta: 18 GWEI ja Etherin kurssi: 3211 euroa

Taulukko 2. Transaktiokustannukset

Operaatio	Käytetty kaasu	Hinta euroissa
Älysopimuksen luonti	1505955	87,06
Lääkärin rekisteröinti	44973	2,60
Potilaan rekisteröinti	47989	2,77
Potilastietojen lisäys	211215	12,21
Potilastietojen luku	0	0

5.2 Älysopimuksen toteutus

Ehdotetussa potilastietojärjestelmässä potilastietojen hallinta toteutetaan Ethereum älysopimuksella. Solidity-kielellä kirjoitettu älysopimus muodostaa järjestelmän rungon ja helpottaa terveydenhuollon ekosysteemin eri yksiköiden välistä vuorovaikutusta. Seuraavassa käydään läpi älysopimuksen toiminnallisuus:

- Potilaan ja lääkärin rekisteröinti

  Lääkärit voivat lisätä järjestelmään uusia potilaita **lisaaPotilas** funktiolla. Kun lisäys on onnistunut, lähetetään tapahtuma **PotilasLisatty**, joka osoittaa uuden potilaan rekisteröinnin. Lääkärit voivat myös rekisteröidä itsensä järjestelmään **lisaaLaakari** funktiolla, joka lähettää **LaakariLisatty** tapahtuman onnistuneen rekisteröinnin jälkeen.

- Potilastietojen lisääminen

  Lääkärit, jotka tunnistetaan heidän yksilöllisistä Ethereum osoitteistaan, voivat lisätä potilastietoja **lisaaTallenne** funktiolla. Tämä funktio hyväksyy parametreja, kuten **cid**, **tiedostoNimi** ja potilaan Ethereum osoitteen (**potilasId**). Potilastietojen lisäämisen yhteydessä lähetetään **TallenneLahetetty** tapahtuma, joka ilmaisee onnistuneen lisäyksen tapahtuneen.

- Pääsynvalvonta ja valtuutus

  Muunnosoperaatioita, kuten **lahettajaOn**, **potilasOn** ja **lahettajaOnLaakari**, käytetään pääsynvalvonnan toteuttamiseen. Sillä varmistetaan, että vain valtuutetut yksiköt voivat suorittaa tiettyjä toimia järjestelmässä. Esimerkiksi **lahettajaOnlaakari** rajoittaa tietyt toiminnot vain rekisteröityneille lääkäreille.

- Potilastietojen hakeminen

  Potilaat ja valtuutetut entiteetit voivat hakea potilastietoja käyttämällä **haeTallenteet** funktiota, joka palauttaa potilaan sairaushistoriaa vastaavan **Tallenne** rakenteen.

- Roolien tunnistaminen

  LahettajanRooli funktion avulla mikä tahansa entiteetti voi määrittää roolinsa järjestelmässä Ethereum osoitteen perusteella.

  Älysopimus mahdollistaa luotettavat, läpinäkyvät ja jäljitettävät transaktiot hyödyntämällä Ethereumin lohkoketjun hajautettua luonnetta. Älysopimuksen toteutus helpottaa potilaiden ja terveydenhuollon tarjoajien välistä vuorovaikutusta, mikä edistää avoimuutta ja vastuullisuutta sähköisten terveystietojen hallinnoinnissa.

5.2.1 Älysopimuksen algoritmi

Alla olevassa kuvassa 11 on ehdotetun älysopimuksen algoritmi.

```
contract Potilastietojarjestelma {

  struct Tallenne {
    address potilasId;
    address laakariId;
    string tiedostoNimi;
    string cid;
    uint256 timestamp;
  }

  struct Laakari {
    address id;
  }

  struct Potilas {
    address id;
    Tallenne[] tallenteet;
  }

  mapping (address => Laakari) public laakarit;
  mapping (address => Potilas) public potilaat;

  event LaakariLisatty(address laakariId);
  event PotilasLisatty(address potilasId);
  event TallenneLisatty(string cid, address potilasId, address laakariId);

  modifier lahettajaOn {
    require(laakarit[msg.sender].id == msg.sender || potilaat[msg.sender].id == msg.sender, "Lahettajaa ei ole");
    _;
  }

  modifier potilasOn(address potilasId) {
    require(potilaat[potilasId].id == potilasId, "Potilasta ei ole");
    _;
  }

  modifier lahettajaOnLaakari {
    require(laakarit[msg.sender].id == msg.sender, "Lahettaja ei ole laakari");
    _;
  }

  function lisaaLaakari() public {
    require(laakarit[msg.sender].id != msg.sender, "Laakari on jo olemassa.");
    laakarit[msg.sender].id = msg.sender;

    emit LaakariLisatty(msg.sender);
  }

  function lisaaPotilas(address _potilasId) public lahettajaOnLaakari {
    require(potilaat[_potilasId].id != _potilasId, "Potilas on jo olemassa.");
    potilaat[_potilasId].id = _potilasId;

    emit PotilasLisatty(_potilasId);
  }

    function lahettajanRooli() public view returns (string memory) {
    if (laakarit[msg.sender].id == msg.sender) {
      return "laakari";
    } else if (potilaat[msg.sender].id == msg.sender) {
      return "potilas";
    } else {
      return "tuntematon";
    }
  }

  function lisaaTallenne(string memory _cid, string memory _tiedostoNimi, address _potilasId)
    public lahettajaOnLaakari potilasOn(_potilasId) {
    Tallenne memory tallenne = Tallenne(_cid, _tiedostoNimi, _potilasId, msg.sender, block.timestamp);
    potilaat[_potilasId].tallenteet.push(tallenne);

    emit TallenneLisatty(_cid, _potilasId, msg.sender);
  }

  function haeTallenteet(address _potilasId)
    public view lahettajaOn potilasOn(_potilasId) returns (Tallenne[] memory) {
    return potilaat[_potilasId].tallenteet;
  }

  function potilasOlemassa(address _potilasId)
    public view lahettajaOnLaakari returns (bool) {
    return potilaat[_potilasId].id == _potilasId;
  }
}
```

Kuva 11. Älysopimuksen algoritmi

5.3 Simulaation parannusehdotukset

Tässä osassa käsitellään Ethereum pohjaista EHR suunnitelmaa, jonka toteutukseen käytettiin Ganachea. Käytetyssä menetelmässä on rajoituksia, jonka takia on syytä tarkastella, miten käytännön tasolla toteutettaisiin optimaalinen testisuunnitelma ja turvallisuusanalyysi järjestelmästä noudattaen parhaita menetelmiä ja metodeja. Suorituskyvyn testaus on tärkeä vaihe, jotta voidaan valmistautua varsinaiseen käyttöönottotilanteeseen. Sitä käytetään mahdollisten pullonkaulojen tunnistamiseksi, resurssien käytön optimoimiseksi ja saumattoman toiminnan varmistamiseksi.

5.3.1 Testisuunnitelma

Alla esitetyssä testaussuunnitelmassa on jäsennelty lähestymistapa lohkoketjupohjaisen potilastietojärjestelmän suorituskyvyn ja turvallisuusnäkökohtien arviointiin. Näitä vaiheita noudattamalla pyritään saamaan tietoa järjestelmän skaalautuvuudesta, eheydestä ja luottamuksellisuudesta. Testausprosessilla arvioidaan järjestelmän valmiutta ja tunnistetaan parannusta vaativia kohteita.

1. Tavoite: Tavoitteena on arvioida järjestelmän skaalautuvuutta, luotettavuutta ja responsiivisuutta vaihtelevien verkko-olosuhteiden ja transaktiokuormien alaisuudessa.
2. Laajuus: Suorituskykytestauksessa keskitytään arvioimaan järjestelmän kykyä käsitellä transaktioita, tiedonhakua, ja tallenteiden lisäämistä. Testiympäristössä simuloidaan käytännön verkko-olosuhteita Goerli, Sepolia ja Rinkeby Ethereum-testiverkkojen avulla.
3. Skenaariot: Potilaan rekisteröinti: emuloi terveydenhuollon tarjoajien suorittamaa uusien potilaiden rekisteröintiä. Mittaa aika, joka kuluu potilastietojen lisäämiseen ja rekisteröintitoimintojen tarkistamiseen. Tallenteiden haku: simuloi potilastietojen hakuun kuluva aika. Tallenteiden lisääminen: testaa järjestelmän kykyä lisätä uusia

potilastietoja profiileihin. Mittaa uusien potilastietojen lisäämiseen käytettävä kaasu ja transaktioiden läpimeno.

4. Testin suorittaminen: Kuormitustestaustyökalujen käyttö, kuten K6 tai Jmeter. Suorita testiskenaariota kasvavilla transaktiomäärillä järjestelmän kapasiteetin stressitestaamiseksi. Seuraa keskeisiä suorituskykymittareita reaaliaikaisesti seurantatyökalujen avulla ja analysoi testituloksia suorituskyvyn optimointia varten.
5. Mittarit: Huomioi transaktiot sekunnissa (TPS), kaasun käyttö transaktiota kohden, vasteaika, suoritusteho, järjestelmäresurssien käyttö (CPU, muisti).
6. Raportointi: Kokoa testitulokset ja dokumentoi havainnot ja suositukset suorituskyvyn optimoimiseksi.
7. Riskit: Tunnista mahdolliset riskit, kuten verkon ruuhkautuminen, tapahtumahäiriöt ja resurssirajoitteet.

5.3.2 Turvallisuusanalyysi

Kattavalla turvallisuusanalyysillä voidaan lieventää mahdollisia tietoturvariskejä ja varmistaa potilastietojen luottamuksellisuus, eheys ja lainmukaisuus. Seuraavassa osiossa on listattu kattavan turvallisuusanalyysin aspektit ja niiden kuvaukset.

- Lainmukaisuus

  Säädösten noudattaminen: Varmista, että terveydenhuollon tietojen käsittelyä, säilytystä ja siirtoa koskevia asiaankuuluvia säännöksiä ja standardeja noudatetaan, kuten HIPAA tai GDPR.

- Luottamuksellisuus

  Tietojen salaus: Ota käyttöön salaustekniikoita IPFS:n kautta tallennettujen ja siirrettävien arkaluonteisten potilastietojen suojaamiseksi. **Pääsynvalvonta:** Käytönvalvontamekanismi

varmistaakseen, että vain valtuutetut henkilöt, kuten potilaat ja terveydenhuollon henkilökunta, pääsevät käsiksi potilastietoihin.

- Tunnistautuminen

  Käyttäjän todennus: Käytä todennusmekanismeja, joilla varmistetaan järjestelmään pääsevien käyttäjien henkilöllisyys. **Monivaiheinen tunnistautuminen (MFA):** Harkitse MFA:n käyttöä käyttäjätilien turvallisuuden parantamiseksi ja luvattoman käytön estämiseksi. **Älysopimusten valtuuttaminen:** Varmista, että vain valtuutetut käyttäjät voivat suorittaa tiettyjä toimia, kuten lisätä tai päivittää potilastietoja.

- Eheys

  Älysopimusten turvallisuus: Arvioi solidity koodi mahdollisten haavoittuvuuksien varalta, kuten vapaakäyntisyys tai kokonaislukujen ylivuoto. **Tietojen muuttumattomuus:** Varmista ettei potilastietoja voida peukaloida tai muuttaa lohkoketjuun lisäämisen jälkeen. **Transaktioiden eheys:** Varmista, että transaktiot suoritetaan oikein, ja että lohkoketjuun tallennetut tiedot pysyvät johdonmukaisina ja luotettavina.

- Muita huomioita

  Tarkastettavuus: Suunnittele järjestelmä siten, että se mahdollistaa tapahtumien ja tietojen käytön tarkastuksen sekä jäljitettävyyden. **Tietoturvatestaus:** Suorita perusteellinen tietoturvatestaus, mukaan lukien tunkeutumistestaus ja koodin tarkastelu, mahdollisten tietoturva-aukkojen tunnistamiseksi. **Häiriötilanteiden hallinta:** Kehitä ja ota käyttöön menettelyt tietoturvaloukkauksiin, jotta niihin voidaan reagoida nopeasti ja tehokkaasti.

6 Pohdinta

Lohkoketjun hajautettu, muuttumaton ja läpinäkyvä luonne tekee siitä lupaavan teknologian muuttaa terveydenhuoltoa mahdollistaen turvallisen tiedonhallinnan, yhteentoimivuuden ja potilaskeskeisen hoidon. Järjestelmällä on monenlaisia käyttömahdollisuuksia, kuten toimitusketjun hallinnan parantaminen, kliinisten tutkimusten ja lääketieteellisten tietojen hallinta sekä potilaiden yksityisyyden suojaaminen.

Lohkoketjun kokonaisvaltainen hyödyntäminen edellyttää kuitenkin yhteentoimivuuden, sääntelyjen, skaalautuvuuden, transaktio kulujen ja standardeja koskevien kysymysten ratkaisemista. Onnistunut integrointi edellyttää terveydenhuollon ammattilaisten ja poliittisten päättäjien välistä yhteistyötä. Keskeiseksi haasteeksi osoittautuu myös itse lohkoketju-kehittäjät, sillä kehittäjien määrä ja asiantuntijuus on vähäistä. Toistaiseksi on myös ollut vaikeaa havainnollistaa selkeästi mitä ja miten lohkoketjuteknologia tuo lisäarvoa terveydenhuoltoon.

Tässä opinnäytetyössä suunniteltiin lohkoketjua käyttävä potilastietojärjestelmä. Parantamalla ensiksi potilastietojen hallintaa ja turvallisuutta voidaan avustaa teknologian integroimista myös mahdollisesti muihin terveydenhuollonjärjestelmiin. Opinnäytetyössä järjestelmän testaus jäi rajoittuneeksi, joten jatkoa ajatellen olisi tarpeellista kehittää realistinen simulaatio ja analyysi, jonka tulosten perusteella voitaisiin paremman arvioida potilastietojärjestelmän käyttöönottoa ja mahdollisesti vaihtoehtoisia lohkoketjualustoja.

Yhteenvetona voidaan todeta, että lohkoketju on verrattain uusi sekä nopeasti kehittyvä teknologia, ja terveydenhuolto on erittäin vaativa ala, jonka seurauksena laajempi muutos tulee vaatimaan vielä aikaa.

Lähteet

Alder, S. (2024). 40 % of Malware infections in Healthcare Originate from Cloud Apps. The HIPAA Journal. Viitattu 15.3.2024 https://www.hipaajournal.com/malware-healthcare-cloud-apps/

Antonopoulos, A. M., Wood, G. (2018) Mastering Ethereum. O'Really Media.

Basil, N., Ambe, S., Ekhator, C., & Fonkem, E. (2022) Health Records Database and Inherent Security Concerns: A Review of the Literature

Berentsen, A., Schär, F. (2018) A Short Introduction to the World of Cryptocurrencies

Ethereum. (n.d.) Consenus mechanisms. Viitattu 22.3.2024 https://ethereum.org/en/developers/docs/consensus-mechanisms/

Ethereum. (n.d.) Introduction to dapps. Viitattu 22.3.2024 https://ethereum.org/en/developers/docs/dapps/

Ethereum. (n.d.) Introduction to smart contracts. Viitattu 22.3.2024 https://ethereum.org/en/smart-contracts/

Ethereum. (n.d.) Smart contract security. Viitattu 22.3.2024 https://ethereum.org/en/developers/docs/smart-contracts/security/

Ethereum. (n.d.) What is Ethereum. Viitattu 22.3.2024 https://ethereum.org/en/what-is-ethereum/

Euroopan komissio (n.d.) Yleinen tietosuoja-asetus https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Ghosh, P., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. (2023) Blockchain Application in Healthcare Systems: A Review

Haleem, A., Javaid, M., Singh, R., Suman, R., & Rab, S. (2021) Blockchain technology applications in healthcare: An overview

Haque, A. K. M. B., & Bhushan, B. (2023) Blockchain for medical insurance: Synthesizing current knowledge and problematizing it for future research avenues

Härdle, W. K., Harvey, C. R., & Reule, R. C. G. (2020) Understanding Cryptocurrencies

Kruse, C., Frederick, B., Jacobson, T., Monticone D.K. (2017) Cybersecurity in healthcare: A systematic review of modern threats and trends

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007. https://www.finlex.fi/fi/laki/alkup/2007/20070159

Lääkärilehti (2020). Tietoturva kiinnostaa nyt kaikkia. Viitattu 23.2.2024 https://www.laakarilehti.fi/ajassa/ajankohtaista/tietoturva-kiinnostaa-nyt-kaikkia/

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021) Security challenges and solutions using healthcare cloud computing

Namasudra, S., Deka, G. C. (2021) Applications of Blockchain in Healthcare. Springer.

Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., & Boutaba, R. (2022) Man-in-the-Middle Attack Mitigation in Internet of Medical Things

Seh, A., Zarour, M., Alenezi, M., Sarkar, A., Agrawal, A., Kumar, R., & Khan, R. (2020) Healthcare Data Breaches: Insights and Implications

Shojaei, P., Vlahu-Gjorgievska, E. (2024) Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review

Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K.-K. R. (2020) Sidechain technologies in blockchain networks: An examination and state-of-the-art review

Stallings, W. (2016) Cryptography and Network Security: Principles and Practice. Pearson.

Tapscott, D., Tapscott, A. (2016) Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Portfolio.

Terveydenhuoltolaki 1326/2010. https://www.finlex.fi/fi/laki/ajantasa/2010/20101326

U.S. Department of Health and Human Services (2021). Blockchain for healthcare. Viitattu 18.3.2024 https://www.hhs.gov/sites/default/files/blockchain-for-healthcare-tlpwhite.pdf

U.S. Department of Health and Human Services (2022). Insider threats in healthcare. Viitattu 3.3.2024 https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf

Ukyab, K.T. & Beato, F. (2024) Healthcare pays the highest price of any sector for cyberattacks – that's why cyber resilience is key. World Economic Forum. Viitattu 21.2.2024 https://www.weforum.org/agenda/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/

Valvira (n.d.). Sosiaali- ja terveydenhuollon tietojärjestelmät. Viitattu 23.2.2024 https://valvira.fi/sosiaali-ja-terveydenhuollon-tietojarjestelmat

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017) Comprehensive study of symmetric key and asymmetric key encryption algorithms

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends