Lauri Miettinen

**KLASSISEN AUTON ELINKAAREN SEURANTA ÄLYKKÄÄLLÄ SOPIMUKSELLA**

**KLASSISEN AUTON ELINKAAREN SEURANTA ÄLYKKÄÄLLÄ SOPIMUKSELLA**

Lauri Miettinen

Opinnäytetyö

Kevät 2017

Kone- ja tuotantotekniikan koulutusohjelma

Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu

Koulutusohjelma, suuntautumisvaihtoehto

Tekijä(t):

Opinnäytetyön nimi:

Työn ohjaaja(t):

Työn valmistumislukukausi ja -vuosi: Sivumäärä:60 + 5 liitettä

Tiivistelmä on suppea, itsenäinen esitys, joka antaa lukijalle kuvan tehdystä työstä. Se kirjoitetaan sitten, kun työ on valmis. Tiivistelmä kirjoitetaan täydellisin virkkein ja passiivimuodossa. Siinä selostetaan lyhyesti työn aihe, tavoitteet, työn keskeisin toteutustapa ja olennaiset tulokset.

Sisältö jakaantuu yleensä kolmeen kappaleeseen:

1. työn aihe ja tavoitteet

2. menetelmät, toteutustapa ja eteneminen

3. tulokset ja esitetyt johtopäätökset.

Tiivistelmän tulee mahtua yhdelle sivulle rivivälillä 1.

Korvaa nämä tekstit omillasi.

Asiasanat: x, x, x

(Kirjoita 3–7 kpl työtäsi kuvaavaa asiasanaa*.* Käytä hyväksesi esimerkiksi yleistä suomalaista asiasanastoa YSA, <http://onki.fi/fi/browser/overview/ysa>.)

ABSTRACT

Oulu University of Applied Sciences

Degree programme, option

Author(s):

Title of thesis:

Supervisor(s):

Term and year when the thesis was submitted: Pages: 60 + 5 appendices

Vieraskielinen tiivistelmä (Abstract) tehdään työn tilaajan niin vaatiessa tai osaston käytänteiden mukaisesti. Sen ei tarvitse olla suora käännös suomenkielisestä tiivistelmästä, vaan sen voi kirjoittaa kansainväliselle lukijalle.

Remember to include the following in the abstract:

Why – background for the thesis, assigner

What – objective of the thesis

How – background knowledge applied, research methods, material used

Achievements – main results

Exploitability – conclusions, development proposals, further measures

The length of the abstract is 1 page.

Keywords: x, x, x

(List 3–7 keywords that describe your thesis. Use for example keywords from the following controlled vocabulary thesauri:

MeSH <http://www.yso.fi/onto/mesh/conceptscheme>

Agriforest <http://www-db.helsinki.fi/agri/agrisanasto/Welcome_eng.html>

Helecon <http://helecon3.hkkk.fi/helevoc/?lang=eng&dbname=MIX>)

ALKULAUSE

Raportissa voi olla alkusanat, joissa kiitetään toimeksiantajaa, ohjaajia ja mahdollisesti muita tukijoita tai avustajia. Alkusanat voi sisältää lyhyesti myös muuta työhön liittyvää, lukijaa kiinnostavaa tietoa, joka ei muuten tule raportissa esiin. Alkusanat päivätään ja allekirjoitetaan.

Korvaa nämä tekstit omillasi.

SISÄLLYS

Contents

[1 JOHDANTO 7](#_Toc484161412)

[2 TEKNIIKKA 9](#_Toc484161413)

[2.1 Lohkoketju 9](#_Toc484161414)

[2.2 Älykkäät sopimukset 9](#_Toc484161415)

[3 SUUNNITTELU JA KÄYTTÖTAPAUKSET 11](#_Toc484161416)

[3.1 Kuvaus käyttötapauksista 11](#_Toc484161417)

[3.2 Lohkoketjun hyöty sovelluksessa 12](#_Toc484161418)

[4 OHJELMISTO 13](#_Toc484161419)

[4.1 Työn kannalta oleellinen ohjelmisto 13](#_Toc484161420)

[4.1.1 Ethereum-alusta 13](#_Toc484161421)

[4.1.2 Ethereum-virtuaalikone 13](#_Toc484161422)

[4.1.3 Solidity-kääntäjä 13](#_Toc484161423)

[4.1.4 Web3-kirjasto 14](#_Toc484161424)

[4.2 Ohjelmointityössä käytetty ohjelmisto 14](#_Toc484161425)

[4.2.1 Browser Solidity 14](#_Toc484161426)

[4.2.2 TestRPC 14](#_Toc484161427)

[4.2.3 Truffle-sovelluskehys 15](#_Toc484161428)

[4.2.4 Meteor 15](#_Toc484161429)

[4.3 Muu työhön liittyvä ohjelmisto 15](#_Toc484161430)

[4.3.1 GoEthereum (geth) 15](#_Toc484161431)

[4.3.2 Ethereum Wallet 16](#_Toc484161432)

[5 TYÖN KULKU 17](#_Toc484161433)

[6 LOPPUTULOKSET 19](#_Toc484161434)

[6.1 Toteutuneet käyttötapaukset 19](#_Toc484161435)

[6.2 Toteutumattomia käyttötapauksia 21](#_Toc484161436)

[7 ARVIO TEKNIIKASTA 24](#_Toc484161437)

[8 LOPPUSANAT 27](#_Toc484161438)

# JOHDANTO

Lohkoketjutekniikka sai alkunsa vuonna 2009, kun Satoshi Nakamoto kirjoitti paperin, jossa hän ehdotti tietomallin puolueettoman valuutan luomisesta. Nykyään valuutta liikkuu pankin tai muun laitoksen kautta. Bitcoinin idea oli luoda valuutta, josta ei ole vastuussa kukaan keskitetty taho, jossa maksajan ei tarvitse luottaa keneenkään. Nakamoto suunnitteli hajautetun järjestelmän rahan lähettämiselle ja maksutapahtumien todentamiselle. (1)

Bitcoin- maksut tallennetaan hajautettuun tietokantaan, jota kutsutaan lohkoketjuksi. Kukaan yksi yritys tai yksi taho ei ole vastuussa Bitcoin-maksuista. Kukin maksutapahtuma lähetetään vertaisverkkoon, jossa se todennetaan. Kuka tahansa voi liittää tietokoneensa Bitcoin-verkkoon todentamaan maksutapahtumia. Maksutapahtumat todennetaan menetelmällä, joka vaatii paljon laskentatehoa. Järjestelmän huijaaminen vaatisi hyökkääjältä enemmän laskentatehoa kuin mitä on kaikilla verkossa olevilla rehellisillä osallisilla. Bitcoin-verkkoon hyökkääjän on ainakin teoriassa mahdollista luoda itselleen rahaa, jota hänellä ei oikeasti ole. Käytännössä hyökkääjällä pitäisi silloin olla käytössään enemmän laskentatehoa kuin koko muulla maailmalla. (1.)

Tekniikka herätti maailmalla mielenkiintoa. Nakamoto pohti hajautettua valuuttaa suunnitellessaan, että olisi suunnitellut laajan hajautetun ohjelmointikielen lohkoketjuille, mutta päättikin tehdä yksinkertaisemman järjestelmän, sillä ymmärsi tekniikan olevan kokeellinen ja haastava luonteeltaan. (2.)

Siitä Vitalik Buterin keksi tehdä Ethereumin, sovellusalustan, jonka sovellukset toimivat lohkoketjun avulla (3.) Kenties joku parempi lähde tähän. Ehkä se alkuperäinen Buterinin paperi?

Lohkoketju on arvokkaan tiedon tallentamiseen perustuva järjestelmä. Bitcoinin tapauksessa arvokas tieto on varallisuus ja valuutta. Klassiset autot ovat arvokkaita. Niistä voidaan käydä satojen tuhansien, ja joskus jopa miljoonien eurojen kauppoja. Autoharrastajat kokevat, että autot ovat maansa kulttuurille merkityksellisiä, sillä kussakin klassisessa autossa on viitteitä aikansa kulttuurista.

Klassiset autot liittyvät myös liikennöinnin alaan. Liikennöinnin alallakin on paljon tulevaisuuden sovelluksia, joissa voitaisiin hyödyntää lohkoketjuja. Koska tämän työn aihe liittyy oleellisesti myös liikennöintiin, tässä työssä saadut tulokset pätevät myös liikennöinnin alalla.

Autoja huoltaessa huoltotietojen tallennus olisi haviteltava ominaisuus. Sekä tavallisille autoille, että klassisille autoille. Tavallisilla autoilla huoltotietoja voivat hyödyntää vakuutusyhtiöt, huoltoyhtiöt, sekä auton omistajat.

Klassisia autoja on huollettava, sillä ne voivat olla kymmeniä vuosia vanhoja, ja niiden osat kuluvat väistämättä. Lohkoketjuun tallennettua tietoa on vaikea muokata jälkeenpäin. Jos klassisen auton huoltotiedot ja käyttötilastot (kilometrimittari) tallennettaisiin lohkoketjuun, auton omistaja voisi vakuuttaa huutokaupoissa ostajan autonsa arvosta.

Nykyään älykkäät sopimukset eivät vielä ole lyöneet läpi maailmanlaajuisille markkinoille. Lohkoketjutekniikkaa tutkitaan vielä yliopistoissa. Älykkäitä sopimuksia ei juurikaan käytetä kaupallisesti. (viite)

Tässä työssä pohditaan liiketoimintamalli ja käyttötapaukset lohkoketjutekniikkaa hyödyntävälle sovellukselle. Tavoite oli luoda Ethereum -älykäs sopimus, jota voitaisiin hyödyntää klassisen auton elinkaaren seurantaan.

Toinen osa työtä oli luoda web-käyttöliittymä, jolla lohkoketjuun tehtäviä merkintöjä voi tehdä ja tarkastella. Tässä työssä kuvaillaan työn suunnittelusta, toteutuksesta ja lopputuloksesta.

Työn tilaaja on Hilla-ohjelma, joka edesauttaa tulevaisuuden tekniikoiden tutkimusta ja kehitystä Suomessa. Työssä oli tavoitteena tehdä sovellus, jonka voi esitellä yhdellä tietokoneella, ja joka näyttää havainnollisesti, mitä älykkäillä sopimuksilla ja lohkoketjuilla voidaan tehdä tulevaisuudessa.

# TEKNIIKKA

## Lohkoketju

Selitä eri tyyppisistä solmuista. Mikä on miner node (5.)

Lohkoketju on vertaisverkossa oleva tietokanta, joka on täynnä tiedonsiirtotapahtumia. Lohkoketjutietokannan tiedonsiirtotapahtumia (transaction) voi ylläpitää ketkä tahansa maailmassa. (7.)

Kuka tahansa voi ladata lohkoketjun kopion tietokoneellensa. Kuka tahansa voi tehdä omasta tietokoneestaan louhijasolmun, joka pyrkii laskemaan uusia lohkoja ja siten todentamaan tiedonsiirtotapahtumia.

Koska samasta lohkoketjusta on kopioita lukemattomilla tietokoneilla. Tämäkin piirre tekee lohkoketjun hakkeroinnista käytännössä hyvin vaikeaa. Jos hyökkääjä haluaisi muunnella ketjussa olevia maksutapahtumia, hänen täytyisi silloin murtautua yhtäaikaisesti kaikkiin tietokoneisiin maailmassa, joissa on kopio lohkoketjusta. (7.)

Kukin tiedonsiirto tallentuu lohkoon. Yhdessä lohkossa on monia tiedonsiirtotapahtumia. Kukin uusin lohko linkittyy edelliseen lohkoon.

## Älykkäät sopimukset

Ethereumin perustaja, Vitalik Buterin, puhuu käsitteestä hajautettu applikaatio (Decentralized Application, eli dapp). (Lähteeksi se lohkoketjukirja)

Bitcoin-verkossa tiedonsiirtoa ovat bitcoin-maksut. Jokaisella tiedonsiirrolla on lähettäjän tili, vastaanottajan tili, sekä siirretty rahasumma. Ethereum-verkossa on näiden lisäksi myös dataa. (lähteeksi ehkä solidity-dokumentaatio)

Ethereum-alusta on kuin tietokone, kuin käyttöjärjestelmä, joka hyödyntää lohkoketjua. (9.)

(15)

Hajautettu sovellus voi käyttää lohkoketjua hyödykseen.

Solidity on suosituin Ethereum älykkäiden sopimusten kirjoitusta varten (15.) Muita kieliä ovat LLL ja Serpent.

Hajautetuissa sovelluksissa on monia hyötyjä verrattuina perinteisiin, keskitettyihin sovelluksiin. Yksi hyöty on se, että ne eivät koskaan ole pois käytöstä. Perinteiset palvelimet voivat kaatuilla palvelinvikojen takia. Hajautettu sovellus ei voi kokonaan poistua toiminnasta, elleivät kaikki vertaisverkon solmut lopeta toimintaansa yhtä aikaa. (15)

Älykkäillä sopimuksilla ei ole ylläpitokustannuksia. Hajautettu sovelluksen palvelinpuoli on vertaisverkossa. Yhdelläkään verkon solmulla ei täysin hallitse dappia.

Nämä ominaisuudet yhdessä tekevät älykkäistä sopimusta mielenkiintoisia yrityksille, jotka etsivät liiketoiminnassaan uusia tekniikan innovaatioita.

Ethereumin sivujen mukaan Ethereum on hajautettu alusta, joka ajaa älykkäitä sopimuksia.

Ei pidä kuvitella että Ethereum on ainoa laatuaan. Hajautettuja sovelluksia voi tehdä ties miten (13) Hajautettuja sovelluksia on ollut olemassa jo jonkin aikaa. Vertaisverkkosovellukset eivät sinänsä ole mitään ihmeellisiä. Onhan tuo bit comet olemassa. Esim windows-päivitykset, ja monien muiden ohjelmistojen päivitykset tulevat vertaisverkossa. (18.)

Ethereum-virtuaalikone on Turing-täydellinen. Alustalla voi ajaa minkä tahansa protokollan, missä tahansa lohkoketjussa. Ethereum-alusta ei tarvitse vain tietyllä tekniikalla toteutettua lohkoketjua, vaan alusta voi hyödyntää minkä tahansa mallista lohkoketjua, mikä saatetaan kehittää tulevaisuudessa. Ethereum-virtuaalikone ei ole riippuvainen mistään tietystä ohjelmointikielestä, eikä virtuaalikoneen ajama koodi ole riippuvainen Soliditystä. Ethereum ei tarvitse mitään tiettyä tiedonsiirtoprotokollaa ollakseen yhteydessä vertaisverkkoon. Nämä periaatteet olivat taustalla, kun Buterin suunnitteli Ethereum-alustaa. (16)

Turing-täydellisyys tarkoittaa sitä, että ohjelmointikielellä voi ratkaista minkä tahansa laskennallisen ongelman. Ethereum on Turing-täydellinen, joten Ethereum-virtuaalikoneella ei ole mitään loogisia rajoitteita liittyen siihen, mitä sillä voi tehdä. Turing-täydellistä ohjelmointikieltä rajoittaa ainoastaan tietokoneen muistin määrä. (17)

Yhdessä vaiheessa ihmiset alkoivat kehittämään hajautettua alustaa Bitcoinin päälle. Näille alustoille kehitettiin tukia monen eri tyyppisille tiedonsiirtotapahtumille. Kaikesta huolimatta, niidenkin rajat tulivat aikanaan vastaan, jolloin täytyi taas kehittää uusia tiedonsiirtotapahtumia.

Omaa tulkintaa: Vaikka tulevaisuudessa romutettaisiin TCPIP, Ethereum ei menisi mäsäksi.

# SUUNNITTELU JA KÄYTTÖTAPAUKSET

## Kuvaus käyttötapauksista

Auton omistajalla on käytössään auton elinkaarta seuraava älykäs sopimus. Auton omistajan tavoitteena on kerätä auton älykkääseen sopimukseen merkintöjä auton elinkaaressa tapahtuneista merkityksellisistä tapahtumista. Tällaisia tapahtumia voivat olla esimerkiksi auton huoltotoimenpiteet, kilpailuvoitot ja asiantuntija-arviot. Merkintöjen tavoite on vakuuttaa tuleva ostaja auton arvokkuudesta. Tässä työssä merkinnöistä käytetään nimeä *kohokohta*, eli *highlight*.

Ajatuksena verkkosovelluksessa on, että kuka tahansa ihminen maailmassa voisi mennä auton älykkään sopimuksen kotisivuille tarkastelemaan auton nykytilaa, siinä olevia kohokohtamerkintöjä ja historiaa.

Ulkopuoliset käyttäjät voivat tehdä verkkosovelluksella kohokohtapyyntöjä (highlight request) älykkääseen sopimukseen. Kohokohtapyynnön voisi esimerkiksi tehdä auton korjannut mekaanikko tai asiantuntija, joka tekee auton autenttisuudesta ja kunnosta arvion. Kohokohtapyynnön tekijä voi pyytää pienen rahallisen korvauksen vaivannäöstä. Esimerkiksi auton korjaava mekaanikko voisi tehdä kohokohtapyynnön, jossa lukee ”Huolsin tämän auton Välivainion huoltoasemalla.”, ja pyytää lomakkeen täyttämisen vaivannäöstä viisi euroa. Lomakkeen täyttämiseen kuluu muutama minuutti, mutta sekin vaatii pientä vaivannäköä. Ihmiset ovat suostuvaisempia muutaman minuutin vaivannäköön, jos siitä saa pienen rahallisen korvauksen.

Kukin kohokohtapyyntö voi maksaa auton omistajalle useita euroja tai kymmeniäkin euroja per merkintä. Kumminkin merkinnät voivat todistaa auton arvokkuuden. Huutokaupassa tarjouksen tekijä saattaa tehdä suuren tarjouksen johtuen merkinnöistä jotka ovat lohkoketjussa. Tällöin auton myyjän maksamat kymmenien eurojen summat maksavat itsensä moninkertaisesti takaisin.

Lisäksi kuka tahansa ihminen maailmassa voisi tehdä tarjouksen autosta. Kaikki tarjoukset ovat julkisia, ja kaikki pystyvät tarkastelemaan niitä. Auton omistaja voi hyväksyä tarjouksen, jolloin hän voi toimittaa auton ostajalle. Sopimuksen omistajuusoikeus siirtyy autokaupan yhteydessä.

## Lohkoketjun hyöty sovelluksessa

Mitä hyötyä on juuri hajautetulla sovelluksella? Tämän sovelluksen voisi kehittää perinteisenä palveluna, joka toimii tavallisella palvelimella, ja jonka merkinnät tallennetaan perinteiseen tietokantaan. Lohkoketjussa ja älykkäissä sopimuksissa on kumminkin piirteitä, joista tämä sovellus voi hyötyä erityisen paljon.

Yksi etu hajautetussa sovelluksessa on tietysti se, että hajautetussa sovelluksessa ei ole lainkaan palvelinkustannuksia. Tavallisessa palvelussa palvelin- ja ylläpitokustannukset täytyy tienata takaisin liiketoiminnalla, kuten mainoksilla. Tämä palvelu on luonteeltaan sellainen, että sitä ei välttämättä käytetä kovin usein, jolloin liiketoiminnan tekeminen voi olla haastavaa. (viite)

Toinen etu on lohkoketjumerkintöjen pitkäikäisyys. Klassisen auton elinkaari voi olla vuosikymmeniä, eivätkä kovin monet yritykset ole olemassa niin kauaa. Jos tavallinen palvelu lopettaa toimintansa, tietokannassa olevat merkinnät voivat kadota. Lohkoketju on paljon pitkäikäisempi, ja koska kopiot tiedoista ovat jokaisella Ethereum-verkon tietokoneella, tiedot eivät voi tuhoutua lopullisesti.

Lohkoketjussa kaikki maksutapahtumat ovat julkisia ja läpinäkyviä. Läpinäkyvyys sopii tämän sovelluksen käyttötapauksiin hyvin. Jos kaikki auton elinkaaressa tulleet tapahtumat ovat julkisia, on huijausten ja väärinkäytösten tekeminen kannattamatonta auton omistajalle. Sovelluksella tehtyjä merkintöjä tarkkailevat voivat tehdä tutkimusta, ja havaita, jos auton elinkaaren merkinnöissä esiintyy väärää tietoa tai ristiriitoja. Sosiaalisen median aikakautena tieto petollisesta auton omistajasta leviää nopeasti ihmiseltä ihmiselle. Maineen menetyksen pelko voi olla suuri. Mikäli tällainen sovellus on oikeasti käytössä tulevaisuudessa, autonomistajat varmasti ymmärtävät, että on kannattavaa pysyä rehellisenä lisättäessä kohokohtia.

# OHJELMISTO

Laita kaikkiin jokin viite mistä sen ohjelman saa ladattua

## Työn kannalta oleellinen ohjelmisto

Kuvaillaan työn kannalta oleellista, sekä työssä käytettyä ohjelmistotekniikkaa.

### Ethereum-alusta

Ethereumiin kuuluu lohkoketju, joka toimii tietokantana. Alustaan kuuluu virtuaalikone, joka on älykkäiden sopimusten ajoympäristö. Ethereum-alusta luo vertaisverkon, jossa käyttäjän koneella käynnissä oleva virtuaalikone on yhteydessä muualla maailmassa oleviin Ethereum-virtuaalikoneisiin. Ethereum-verkko koostuu maailmanlaajuisesti yhteen liittyneiden Ethereum-solmujen vertaisverkosta. Jos Ethereum-verkkoa haluaa käyttää, tulee omalle tietokoneelle käynnistää Ethereum-solmu, esimerkiksi GoEthereum (ks. 3.3.1).

### Ethereum-virtuaalikone

Ethereum-virtuaalikone sisältää Ethereum-koodiajoympäristön. Ethereum-alustan alkuaikoina, yksi Ethereumin perustajista, Gavin Wood, teki teknisen spesifikaation siitä, mitä käskyjä Ethereum-virtuaalikoneen kuuluu toteuttaa (5). Täten Ethereum-virtuaalikoneen voi toteuttaa kuka tahansa, lähes millä tahansa ohjelmointikielellä. Virtuaalikone on tehty esimerkiksi Go-kielellä (ks. 3.3.1), sekä Pythonilla.

### Solidity-kääntäjä

Solidity-kääntäjä kääntää Solidity-kielen Ethereum-tavukoodiksi, jonka Ethereum-virtuaalikone muuntaa konekäskyiksi. Solidity-kieli on hyvin yksinkertainen ja helposti opittava. Se muistuttaa Javascriptiä. Ohjelmoijayhteisö on kehittänyt monia Solidity-kääntäjiä. Yksi kääntäjä on Browser Solidity (ks. 3.2.1). Kääntäjiä on myös Truffle-sovelluskehyksessä sekä Ethereum Wallet -ohjelmassa.

### Web3-kirjasto

Web3 on javascript-kirjasto, joka pystyy lähettämään kutsuja paikalliselle ethereum-solmulle. Web3:n avulla internet-selaimessa olevat sovellukset voivat vuorovaikuttaa Ethereum-verkon kanssa. Web3:sta on olemassa npm-paketti, jonka voi ottaa käyttöön helposti Meteorissa. Kirjasto on hyvin dokumentoitu esimerkkeineen Ethereumin GitHubin wiki-sivuilla. (20)

## Ohjelmointityössä käytetty ohjelmisto

Tässä kuvaillaan ohjelmistoa, jota päädyttiin käyttämään lopullisessa työssä

### Browser Solidity

Browser solidity on selaimessa käytettävä kääntäjä. Javascriptin suorituskyvystä johtuen browser solidity voi olla hidas. Sen etuna on, että se toimii kaikilla tietokoneilla ilman ylimääräisten ohjelmien asennusta.

### TestRPC

TestRPC on node-palvelinsovellus, joka on tehty mukailemaan hyvin tarkasti Ethereum-lohkoketjun toimintaa.

Maksutapahtumien todentaminen tapahtuu testrpc:ssä hyvin nopeasti.

TestRPC:n asentaminen on helppoa Linuxilla, käyttäen Node pakettihallintaohjelmaa (Node package manager, npm). Windowsilla asentaminen on vaikeampaa. Windowsille asentaessa on kannattavaa lukea testrpc-repositorion lueminut (readme) -tiedostossa olevia ohjeita. Kaikki Windows-koneelle tarvittavat resurssit on mahdollista asentaa ilmaisen Microsoft Visual Studio Community Edition -asennuksen yhteydessä.

### Truffle-sovelluskehys

Truffle on Ethereum -älykkäiden sopimusten kehittämistä varten luotu sovelluskehys, jonka on tarkoitus helpottaa Solidity-kielellä älykkäiden sopimusten koodin kirjoittamista. Sovelluskehyksen avulla voi tehdä älykkäiden sopimusten jatkuvaa integraatiota Ethereum-lohkoketjuun. Trufflen avulla voi myös koodata automatisoituja testejä sopimuksille.

### Meteor

Meteor on sovelluskehys, joka yhdistää Node-palvelimen MongoDB -tietokannan hyvin helppokäyttöisesti. Meteor on saanut maailmalla huomiota, koska sen avulla voi tehdä samanaikaisesti verkkosivuja sekä mobiilisovelluksia. Meteoriin on helppo ohjelmoida reaktiivisia käyttöliittymiä, eli tehdä sovelluksesta sellainen, että sen käyttöliittymä näyttää reaaliaikaisesti kaikki päivitykset mitä tulevat tietokantaan. Meteor-sovelluskehyksellä on X seuraajaa githubissa, tehden siitä Y:nneksi suosituimman repositorion.

## Muu työhön liittyvä ohjelmisto

Kuvaillaan muuta ohjelmistoa, joka liittyy työhön, tai käytettiin jossain työn vaiheessa.

### GoEthereum (geth)

Go-kielellä ohjelmoitu Ethereum-virtuaalikone. Tämän työn sovellusta kehittäessä geth-solmua ei juurikaan käytetty, koska kehityksessä käytettiin lähinnä testrpc-testiverkkoa. Geth-solmua tarvittaisiin, jos työssä kehitetty älykäs sopimus haluttaisiin sijoittaa oikeaan Ethereum-verkkoon. (11) (12)

### Ethereum Wallet

Valitettavasti Ethereum Wallet ei toimi testrpc:n kanssa, koska testrpc toteuttaa vain osan kaikista rajapinnoista, joita geth-solmussa on. Ethereum Wallet käyttää rajapintaa signAndSendTransaction, mitä ei ole toteutettu testrpc:ssä.

# TYÖN KULKU

Aloituspalaverin pitämisen jälkeen aloitettiin pohtimaan työn tarkoitusta. Ohjelmistotyön idea keksittiin, siitä tehtiin vaatimusmäärittely, jonka työn tilaaja hyväksyi.

Tutustuttiin Ethereumiin käyttämällä Ethereum Wallet -ohjelmaa. Pystytettiin geth-testiverkko tietokoneelle. ClassicCarChain-älykkään sopimuksen koodaus aloitettiin.

Työskenneltiin geth-testiverkon parissa, kunnes todettiin, että nopeaa, iteroivaa työskentelytapaa varten testiverkko oli liian hidas. Asennettiin testrpc-testiverkko tietokoneelle, jonka jälkeen älykkään sopimuksen suorituskyky näytti paranevan.

Truffle-sovelluskehyksen käyttö aloitettiin. Kokeiltiin automaattisten testejä. Automaattisten testien koodaus oli kumminkin hyvin työlästä, joten niiden kehittämisestä luovuttiin myöhemmin. Työn lopun ajan Trufflea käytettiin lähettämään (deploy) sopimus lohkoketjuun.

Meteor-sovelluskehyksen käyttö aloitettiin. Tehtiin Meteorilla Ethereumiin liittymättömiä harjoitustöitä, jotta kehittämisen perusteet tulisivat tutuiksi.

Älykkään sopimuksen ja Meteor-sovelluksen välisessä rajapinnassa alkoi ilmetä ongelmia, johtuen Solidity-kielen ja virtuaalikoneen teknisistä rajoitteista. Älykästä sopimusta uudelleen koodattiin ja eri ratkaisuja kokeiltiin.

Vastaan tuli ongelma käyttötapauksessa ”vierailijan pitää kyetä näkemään kaikki kohokohdat, mitä autolla on”, sillä Solidity-kielessä ei ole tietorakennetta, jonka kaikki alkiot voisi hakea yhtä aikaa web3-rajapinnan kautta Meteor-käyttöliittymään. Ongelma ratkaistiin tekemällä meteoriin kiertokyselyrakenne, joka hakee yksitellen kaikki alkiot sopimuksesta.

Hyviä ohjelmistosuunnitteluperiaatteita pyrittiin seuraamaan suunnittelemalla sopimus uudelleen siten, että jokainen kohokohtamerkintä olisi Ethereum-lohkoketjussa oma alisopimuksensa, joihin ClassicCarChain-pääsopimus tekisi kutsuja. Yhteyden todentaminen onnistui, eli funktiokutsuja alisopimuksessa pystyy tekemään ainoastaan tietty sopimus. Suunnitelmasta jouduttiin kumminkin luopumaan, koska Ethereum-virtuaalikoneessa sopimus ei voi hakea toisesta sopimuksesta arvoa, jonka pituus on muuttuva. Tällaisia tietueita ovat muun muassa merkkijonot (string), sekä taulukot (array).

Lopuksi tehtiin käyttöliittymää. Ethereum-yhteisön kehittämää dappstyles.styl-tyyliä kokeiltiin. Työssä päädyttiin tekemään oma yksinkertainen css-tyyli.

# LOPPUTULOKSET

Työtä kehitettiin GitHub-repositoriossa, josta sen voi ladata. Lueminut-tiedostossa on ohjeita työn käynnistämistä varten. Kuvassa X on auton omistajan näkymä sovelluksen etusivuilta. Yläpalkissa on sovelluksessa navigointilinkit, oikeassa yläkulmassa aktiivisen tilin vaihtaminen. Yläpalkin alapuolella lomake kohokohdan lisäämistä varten. Sininen laatikko on yksi kohokohta, jossa auton omistaja näkee poistamispainikkeen, sekä tekstikentän, johon voi kirjoittaa syyn merkinnän poistamiselle.



Kuva X. Lopullinen sovellus kohokohtasivulta.

## Toteutuneet käyttötapaukset

* Auton omistaja näkee sovelluksessa eri toimintoja kuin muut käyttäjät.
* Kun käyttäjä käynnistää sovelluksen, hän pystyy vaihtamaan käyttäjätiliään. Kun käyttäjätiliä vaihtaa, käyttöliittymä päivittyy välittömästi näyttämään käyttäjälle ne ominaisuudet ja tiedot, mitä käyttäjällä on oikeus nähdä.
* Autentikaatio tapahtuu Ethereum-verkossa. Kuka tahansa voisi esimerkiksi kutsua verkkosivuilla funktiota, jolla saisi auton omistajuuden (gainOwnership). Tällöin Ethereum-verkossa havaitaan, ettei kutsun lähettänyt tili olekaan auton omistaja, jolloin mitään ei tapahdu.
* Omistaja pystyy lisäämään kohokohtia omaan autoonsa. Kohokohdassa on tietueina muun muassa merkinnän lisäämisaika, viesti ja merkinnän tekijä.
* Omistaja voi poistaa kohokohtamerkintöjä.
* Muut tilit pystyvät lisäämään kohokohtapyyntöjä. He voivat pyytää rahasumman palkkioksi auton omistajalta siitä vaivannäöstä, että he tekivät kohokohtapyynnön.
* Auton omistaja pystyy lähettämään rahaa sopimuksen saldoon omalta tililtään. Kohokohtapyynnön hyväksyessä raha siirtyy sopimuksen saldosta kohokohtapyynnön tekijälle. Jos sopimuksessa ei ole tarpeeksi saldoa, kohokohtapyyntöä ei voi hyväksyä. Tämä rajoite on sovelluksessa Ethereum-alustan turvallisuusrajoitteiden takia.
* Auton omistaja voi nostaa rahaa sopimuksen saldosta.
* Omistaja pystyy hyväksymään kohokohtapyynnön, jolloin se lisätään auton kohokohtien joukkoon. Samalla sopimuksen saldosta siirtyy pyydetty summa kohokohtapyynnön tekijälle.
* Omistaja voi kieltäytyä kohokohtapyynnöstä, jolloin se poistetaan.
* Muu kuin auton omistaja pystyy tekemään tarjouksen autosta.
* Tarjouksen tekijä voi myös poistaa tarjouksensa, jos muuttaa mieltään.
* Auton omistaja voi kieltäytyä tarjouksesta, jolloin se poistuu tarjousten listalta.
* Omistaja pystyy hyväksymään tarjouksen, jolloin sopimus siirtyy ”omistajuus on vaihtumassa” -tilaan. Tässä tilassa sovelluksen etusivuilla näkyy tiedote omistajuuden siirtymisestä kaikille käyttäjille.
* Kun auton omistajuus on vaihtumassa, auton ostaja näkee painikkeen, jolla hän pystyy saamaan sopimuksen omistusoikeudet. Ajatuksena on, että ostaja painaa tästä painikkeesta, kun auto on toimitettu hänelle.
* Painikkeen painamisen jälkeen uusi omistaja saa kaikki käyttöoikeudet, mitä edellisellä omistajalla oli. Edellinen omistaja näkee samat ominaisuudet kuin muutkin tavalliset käyttäjät.
* Jokainen yllä mainittu toiminto tallentaa sopimukseen historiatietomerkinnän (Solidity-kielessä ”event”). Merkintöjä tallentuu myös silloin kun tietueita poistetaan. Historiatietomerkintöjä voi tarkastella kuka tahansa, eikä niitä voi poistaa kukaan.

## Toteutumattomia käyttötapauksia

Varhaisessa työn vaiheessa suunniteltiin roskapostin estojärjestelmä kohokohtapyynnöille. Nykyisessä sovelluksessa yksikin käyttäjä pystyisi lähettämään tuhansia kohokohtapyyntöjä päivässä. Tätä varten kehitettiin työn aikana ominaisuus, jota voisi luonnehtia kohokohtien pyyntöoikeuksiksi (highlight request rights). Tavoitteena oli kehittää järjestelmä, jossa auton omistaja voisi antaa eri käyttäjille oikeudet lisätä kohokohtapyyntöjä. Ominaisuus olisi hyödyllinen esimerkiksi julkisuuden henkilölle, jonka auto on kirjattu sovellukseen. Julkinen auto saa paljon huomiota sosiaalisessa mediassa, jolloin roskaposti voi olla riesa auton omistajalle. Epäsuositun auton omistaja voisi laittaa asetuksen pois päältä, jolloin kuka tahansa käyttäjä voi lähettää kohokohtapyyntöjä. Yhdessä ohjelman versiossa tätä ominaisuutta kehitettiin, mutta kehitys lopetettiin, koska päätettiin, ettei käyttötapauksen demonstroiminen ollut tarpeeksi tärkeää työn tarkoituksen kannalta. Tämä työ toimii vain yhdellä tietokoneella, mutta mikäli sopimus lähetettäisiin varsinaiseen Ethereum-verkkoon, tämä käyttötapaus voisi olla hyödyllistä olla toteutettuna.

Toinen työn alkuvaiheissa suunniteltu käyttötapaus on rahasummista tinkiminen. Olisi mahdollista koodata sopimukseen logiikkaa, jossa auton omistaja voisi tinkiä kohokohtapyynnöstä pyydettyä summaa. Tinkimisen voisi lisätä myös autokaupassa tarjouksen tekijän ja auton omistajan välille. Tästä käyttötapauksesta luovuttiin, koska se on työläs kehittää. Käyttötapaus vaatisi hyvin suunnitellun, hyvin testatun, virheettömän koodin älykkääseen sopimukseen. Maksutapahtumia käsitellessä, raha saattaa kadota ohjelmointivirheen seurauksena. Vaatisi lisäksi selkeän käyttöliittymän Meteor-sovellukseen, jotta käyttäjä ymmärtää, missä vaiheessa rahanvaihto ja tinkimien ovat.

Kolmas toteuttamaton käyttötapaus on historiatietojen suodattaminen ja järjestely. Lopullisessa sovelluksessa kaikki historiatiedot ovat samassa listassa peräjälkeen. Olisi käytettävyyden kannalta parempi, jos listaan voisi lisätä suotimia ja siitä voisi tehdä hakuja.

Neljäs on uusien ajoneuvojen lisääminen Ethereum-verkkoon. Sovellukseen olisi pystynyt lisäämään lomakkeella uuden auton, jolle tehdään uusi sopimus lohkoketjuun. Tätä varten tehtiin käyttöliittymä, jonka pystyy näkemään lopullisessa sovelluksessa. Käyttöliittymää pääsee katsomaan, kun käynnistetyssä sovelluksessa menee sivulle http://localhost:3000/. Toiminnallisuus jätettiin tekemättä. Ominaisuuden toteutus vaatisi Meteor-sovelluksen Javascript-koodin tarkempaa suunnittelua. (Kuva X)



Kuva X. Lomake, jolla uuden sopimuksen voisi lähettää.

Viidentenä suunniteltiin, että huoltotiedot voisi lisätä lomakkeella kohokohtaan. Tämä oli haastava toteuttaa, sillä Solidityssä tuki muuttuvan pituisille tietorakenteille, kuten taulukoille, on ongelmallinen. Tämä käyttötapaus olisi hyvin vakuuttavalla tavalla voinut vakuuttaa älykkäiden sopimusten hyödystä liikennöinnin alalla. Lopulta kumminkin todettiin, ettei käyttötapaus ollut elintärkeä työn tarkoituksen kannalta, eikä sitä toteutettu. Huoltotiedot suunniteltiin koodattavan aluksi vain viitenä huoltotehtävänä, joille kullekin voisi merkata huollon lopputuloksen:

**struct MaintenanceTasks {**

**MaintenanceOutcome engine;**

**MaintenanceOutcome tires;**

**MaintenanceOutcome pedals;**

**MaintenanceOutcome brakes;**

**MaintenanceOutcome interior;**

**}**

**enum MaintenanceOutcome {**

**NotChecked, Checked, CheckedAndFoundFault,**

**FoundFaultAndFixed**

**}**

Kuudentena on tietoturvan puutteet. Lopullisessa sovelluksessa auton myynnissä ja ostossa on joitakin tietoturva-aukkoja. Nykyinen järjestelmä vaatii ostajaa lähettämään koko tarjoamansa summan sopimukseen. Tämä tehdään tarjouksen tekohetkellä. Kymmenien tai satojen tuhansien eurojen ostossa, on epäkäytännöllistä kiinnittää niin suuria rahasummia pitkäksi aikaa. Olisi suositeltavaa, jos sekä ostaja, että myyjä lähettäisivät pienen osuuden kaupasta, esimerkiksi 5%, auton hinnasta sopimukseen. Auton ostaja lähettäisi rahat tarjouspyyntöä tehtäessä, ja myyjä lähettäisi tarjouspyynnön hyväksyessä. Kun molemmilla osapuolilla on rahaa kiinnitettynä sopimukseen, molemmilla on vähemmän motiiveja yrittää petosta autokaupan aikana. Auton myyjä saisi koko kaupan rahat, kun ostaja on hyväksynyt kaupan (Painamalla painiketta ”Olen saanut ajoneuvon. Ota sopimuksen omistajuus”)

Viimeisenä mainittakoon, että nykyisessä järjestelmässä on mahdollista saman käyttäjän tehdä useampi tarjous. Olisi parempi, jos yksi käyttäjä voisi tehdä yhden tarjouksen, jolloin uudempi tarjous yli kirjoittaa vanhan.

# ARVIO TEKNIIKASTA

Truffle on varmasti hyödyllinen projektissa, jossa on tuhansia rivejä Solidity-koodia, sekä suurempi kehitystiimi, jossa ainakin yksi kehittäjä voi kuluttaa aikaa testien koodaamiseen. Tämän laajuisessa työssä Truffle-sovelluskehyksestä saatu hyöty jäi vähäiseksi.

Meteorilla työskentely oli nopeaa ja sujuvaa. Meteorissa hyvä ominaisuus on javascript-koodien yhdistäminen ja universaalisuus koko sovelluksessa. Mallipohjat ja mallipohjien apurifunktiot ovat hyvin monipuolisia. En pidä tästä kappaleesta

Tässä sovelluksessa, sekä kaikissa muissakin Ethereum-sovelluksissa Meteorin reaktiivisuus on hyvin hyödyllinen. Sovelluksessa lohkoketjussa tapahtuvat muutokset näkyvät käyttöliittymässä välittömästi.

Solidity-kieli jätti toivomisen varaa. Kielessä on paljon teknisiä rajoitteita. Osa rajoitteista johtuu ohjelmointikielen vähäisestä kehityksestä. Solidity on tällä hetkellä versiossa 0.4.7. Osa solidity-kielen rajoitteista johtuu Ethereum-virtuaalikoneen rajoitteista. Solidity-kieli on hyvin monipuolinen ja helppokäyttöinen, mutta sitä käyttävien kehittäjien on hyvä olla tietoisia rajoitteista, joita kielessä on. Rajoitteista tietäminen säästää kehitysaikaa, ja vähentää turhan työn ja kokeilujen määrää.

Solidity-kielessä on ollut menneissä versioissa turvallisuusongelmia. Turvallisuusongelmat ovat vaarantaneet koko Ethereum-alustan (4). On mahdollista, että turvallisuusongelmia ilmenee tulevaisuudessakin. Koska Ethereum-verkossa liikkuu rahaliikennettä, turvallisuusongelmat ovat huomattava uhka alustan tulevaisuudelle.

Solidity-kielessä ei voi hakea koko mapping-tietorakenteen kaikkia alustettuja alkioita. Kehittäjän täytyy itse kirjoittaa funktiot koko mappingin alkioiden haulle. Tämä tulee hidastamaan huomattavasti hajautettujen sovellusten (Ensimmäinen kerta, kun sanot tämän sanan. Selitä) kehitystä, niin kauan kuin se on olemassa.

Tässä työssä tehtiin Meteor-sovelluksessa javascript-koodia, joka hakee yksitellen kaikki alkiot mapping-tietorakenteesta. Sen ohjelmoiminen ei ole vaikeaa, mutta sen koodaaminen virheettömästi on silti aikaa vievää. Vaikka mapping-tietorakenteessa on teknisiä rajoitteita, Solidity-kieleen olisi mahdollista kehittää tietorakenne, joka laajentaa mapping-tietorakenteen toiminnallisuutta, ja jossa tässä mainitut ongelmat voisivat olla korjattu. Vaikka tietorakenne olisikin suorituskyvyltään hidas, olisi se silti tärkeä ominaisuus, koska se lisäisi innovaatioiden määrää Ethereum-sovelluksien kehittäjien keskuudessa. Innovaatiot ovat hyvin tärkeitä Ethereumille.

Ei voi kutsua vieraassa sopimuksessa olevaa funktiota, joka palauttaa string-tyyppisen muuttujan. Yhdessä vaiheessa tehtiin ohjelmistosuunnitelma, jossa pyrittiin tekemään kohokohdista omia sopimuksiaan. Kohokohtasopimuksista pääsopimus voisi lukea tietoja. Suunnitelma hylättiin tässä mainitun teknisen rajoitteen takia. String-tyyppisten tietueiden näyttäminen oli ehdoton tämän suunnitelman kannalta.

Solidityssä ei ole tukea useille sopimuksen konstruktoreille. On mahdollista suunnitella ohjelmansa eri tavalla, ja rajoitteeseen voi sopeutua. Joissakin ohjelmissa tämä voi tehdä koodista epäselvää ja vaikeasti luettavaa.

On huomattava puute, että Solidity-koodissa ei ole null-käsitettä. Monissa ohjelmissa kehittäjä haluaisi tehdä funktioita, joka joko palauttaa arvon, kun funktion kutsu onnistuu, mutta palauttaa null silloin kun se ei onnistu. Null-käsite on myös hyödyllinen, kun halutaan tarkistaa, onko muuttujia alustettu.

Ethereum-yhteisö on hieman hajautunut. Kehittäjä, joka haluaa tehdä

Vaikka rajoitteet kuulostavat pieniltä, ne kumminkin rajoittavat suuresti kaikkia mahdollisia käyttötapauksia, mitä Ethereum-alustalla voisi muuten toteuttaa. Rajoitteet tulevat hidastamaan Ethereumin läpimurtoa yleiseen, maailmanlaajuiseen käyttöön. Tästä huolimatta, Soldity-kieltä kehitetään parhaillaan, ja joitakin hyvin oleellisia parannuksia on tehty viime aikoinakin, kuten (?).

Voi olla kannattavaa kertoa EtherSimistä, ja kertoa kuinka käsittämättömän hämmentävää on pysyä mukana Ethereum-ohjelmistokehityksen nykytilanteesta. Aina kaikkea uutta tehdään ja jotain heitetään roskakoriin. Vaikea löytää mikä on uusinta tietoa. Voit laittaa esimerkiksi viitteen siihen uhkapelisovelluksen, jossa kehittäjä turhautui Mist/Ethereum Wallet -sekoiluun, ja dumppasi koko sovelluksen.

Silti kukaan ei voi kieltää Solidity-kielen mahdollisuuksia. Kieli on niin yksinkertainen, että kuka tahansa, jolla on ymmärrystä ohjelmoinnista voi oppia sen. Kielen helppokäyttöisyydellä ja yksinkertaisuudella on suuri merkitys Ethereum-alustan maailmanlaajuisessa läpimurrossa.

# LOPPUSANAT

Työssä oli tavoitteena luoda käytännön sovellus, joka havainnollisesti esittelee, miten tulevaisuudessa voitaisiin hyödyntää älykkäitä sopimuksia. Tätä varten tutustuttiin Ethereum-alustan ohjelmistokehitykseen.

Ethereum-alustaa varten on kehitetty monia helppokäyttöisiä kehitystyökaluja. Solidty-kieli on helppo oppia, vaikka sen ominaisuuksissa on kehitettävää. Solidity-kielen rajoitteet hidastavat kehitystä ja rajoittavat innovaatioita, joita Ethereum -älykkäillä sopimuksilla voi kehittää.

Meteor on hyvin helppokäyttöinen sovelluskehys. Se soveltuu hyvin Ethereum-alustaan pohjautuviin sovelluksien kehittämiseen.

Lohkoketjutekniikan tutkijat puhuvat, että historia voi jakaantua ennen lohkoketjuja olleeseen, ja lohkoketjujen jälkeiseen maailmaan, että lohkoketjut ovat keksintönä yhtä merkityksellinen kuin internet. (19)

Jää nähtäväksi, tuleeko ennustuksesta totta. Elämmekö tulevaisuudessa maailmassa, jossa raha, tavaroiden ja palvelujen korvaukset liikkuvat ihmiseltä ihmiselle, ilman välikäsiä, kaikki käyttäen hajautettuja sovellusalustoja?

LÄHteet

1. <https://bitcoin.org/bitcoin.pdf>
2. <https://www.youtube.com/watch?v=3PdO7zVqOwc>
3. <http://futurethinkers.org/vitalik-buterin-ethereum-decentralized-future/>
4. <https://blog.ethereum.org/2016/11/01/security-alert-solidity-variables-can-overwritten-storage/>
5. <http://gavwood.com/paper.pdf> vaihtoehtoinen linkki: <http://paper.gavwood.com/> Hakupäivä 01.07.2017.
6. <https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html>
7. <https://www.youtube.com/watch?v=4sm5LNqL5j0&t=10s>
8. Building on Bitcoin. By: Aron, Jacob, New Scientist, 02624079, 2/8/2014, Vol. 221, Issue 2955. saatavissa <https://www.ebscohost.com/> (vaatii käyttöoikeuden)
9. <https://ethereum.org/>
10. <http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html#the-evm>
11. <http://ethdocs.org/en/latest/ethereum-clients/choosing-a-client.html#why-are-there-multiple-ethereum-clients>
12. <http://ethdocs.org/en/latest/ethereum-clients/go-ethereum/index.html>
13. <https://youtu.be/Fjhe0MVRHO4?t=9m3s>
14. <https://youtu.be/3PdO7zVqOwc?t=8m30s> Mikä on lohkoketju. Alkaen 8:30-10:40
15. Building Blockchain ProjectsBy: Narayan Prusty Publisher: Packt Publishing Pub. Date: April 27, 2017 Saatavilla: <http://proquest.safaribooksonline.com/> (vaatii käyttöoikeuden)
16. Blockchain By: Melanie Swan Publisher: O'Reilly Media, Inc. Pub. Date: February 9, 2015Print ISBN-13: 978-1-4919-2049-7 Saatavilla safaribooks (vaatii käyttöoikeuden) Kappaleen nimi: Ethereum: Turing-Complete Virtual Machine
17. <https://www.youtube.com/watch?v=RPQD7-AOjMI> Turing Complete – Computerphile
18. <https://youtu.be/Fjhe0MVRHO4?t=1m54s> 1:54-8:53 D2P3 - TNABC 2015 - VITALIK BUTERIN FOUNDER ETHEREUM - Bitcoin 2.0 - Ideas and Applications
19. <https://www.youtube.com/watch?v=40ikEV6xGg4> Block chain demystified
20. <https://github.com/ethereum/wiki/wiki/JavaScript-API> Web3 JavaScript app API