VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Ville Övermark

Ethereum-opas piensijoittajalle

Liiketalous
2019

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Ville Övermark
Opinnäytetyön nimi	Ethereum-opas piensijoittajalle
Vuosi	2019
Kieli	Suomi
Sivumäärä	29
Ohjaaja	Päivi Rajala

Aiheeni opinnäytetyöhön valikoitui, koska kryptovaluutat on ajankohtainen aihe ja olen kiinnostunut kryptovaluutoista ja seurannut kryptovaluuttoja, niiden markkinoita ja kehitystä useamman vuoden ajan. Opinnäytetyöni tarkoitus on selvittää Ethereum-kryptovaluuttaa, jotta siitä kiinnostuneet sijoittajat saavat tietoa siitä, mihin kryptovaluuttaa voidaan käyttää, minkälaisella tekniikalla sitä käytetään ja kuinka sitä hankitaan.

Opinnäytetyöni alkaa kryptovaluutan historiasta, jonka jälkeen selvitetään sen tärkeitä ominaisuuksia sekä termistöä aiheeseen liittyen. Lähteet ovat pääasiallisesti internetlähteitä, koska aiheena kryptovaluutat on suhteellisen uusia, eikä niistä ole kirjoitettu juurikaan kirjoja.

Tutkimuksessa havainnollistetaan piensijoittajan tai yrittäjän mahdollisuuksia hyödyntää Ethereumin ominaisuuksia sovelluksien kehittämisessä, älykkäiden sopimuksien avulla tai puhtaasti sijoitusmielessä. Tämän opinnäytetyön tuloksena syntyy opas, josta selviää miten kryptovaluutta Ethereumiin sijoitetaan, mistä sitä hankitaan ja kuinka sitä säilytetään sitä turvallisesti.

Avainsanat Kryptovaluutta, Ethereum, Lohkoketju, Sovellukset

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Ville Övermark
Title	An Ethereum-Guide for Small Investors
Year	2019
Language	Finnish
Pages	29
Name of Supervisor	Päivi Rajala

The subject for this thesis was chosen mainly because cryptocurrencies have been a hot topic for several years now and I have been following its markets and new projects being developed to this market for some time. The objective of this thesis was to study and introduce Ethereum in detail, so that small investors who might be interested in this field can learn how to use Ethereum, what the technology behind it is and how to obtain it.

The thesis starts by introducing the history of cryptocurrencies in general, after which the important features of Ethereum are reviewed and the terminology related to the topic is explained.

The research material was mainly obtained from the internet because the subject of cryptocurrencies is relatively new and there are few books written about the subject, so it's difficult to find any material in the libraries. In the study the aim was that whether you were a small investor or an entrepreneur, you can take advantage of the features that Ethereum brings, either through application development, smart contracts or as an investment. The aim is that after reading this thesis the reader can have a basic understanding on Ethereum.

Keywords Cryptocurrency, Ethereum, Blockchain, Dapps

SISÄLLYS

KUVALUETTELO

1 JOHDANTO

Opinnäytetyön tarkoituksen on perehtyä Ethereum-kryptovaluuttaan ja selvittää sen toimintaperiaatetta, käyttötarkoitusta ja tekniikkaa. Työn aihe valikoitui, koska kryptovaluutat on ajankohtainen aihe, varsinkin Bitcoin. Medialta ja yleisöltä jää usein monta muuta potentiaalista kryptovaluuttaa Bitcoinin varjoon, siksi halusin tehdä tutkimuksen Ethereumista sen ominaisuuksien ja rakenteiden tuomat mahdollisuudet ovat todella mielenkiintoiset ja niitä voidaan soveltaa useaan eri tarkoitukseen. Ethereumia voidaan käyttää sekä ns. valuuttana, nopeiden ja halpojen transaktioiden ansiosta, sekä sovelluksien kehitysalustana, jolloin kolmas osapuoli pystyy kehittämään Ethereumin lohkoketjun päälle omia sovelluksiaan.

Tämän opinnäytetyön tarkoituksena on tehdä kattava opas siitä, mitä Ethereum on ja mitä se sisältää, käsitellä mahdollisimman kattavasti termistöä ja selvittää, mitä Ethereumilla voidaan tehdä.

Tutkimusmenetelmäksi olen valinnut laadullisen tutkimuksen. Tutkimuksessa selvitetään Ethereum-kryptovaluutan ominaisuuksia, mahdollisuuksia ja merkitystä.

Lisäksi tutkimuksessa verrataan Etheriumia Bitcoiniin. Tarkoituksena on, että tämän opinnäytetyön luettuaan lukija ymmärtää, mikä Ethereum on, mitä se sisältää ja mitä sillä voidaan tehdä.

2 KRYPTOVALUUTTA

Kryptovaluutta on virtuaalinen valuutta, joka on suunniteltu toimimaan vaihdon välineenä. Kryptovaluutat käyttävät salausta varmistaakseen ja tarkistaakseen tapahtumia sekä hallitsemaan tietyn kryptovaluutan uusien yksiköiden luomista. Pohjimmiltaan kryptovaluutat ovat rajoitettuja merkintöjä tietokannassa, joita kukaan ei voi muuttaa eikä manipuloida.

Digitaalisia valuuttoja yritettiin luoda jo 90-luvulla teknologian kehittyessä hurjaa vauhtia. Näistä tunnetuimpia valuuttoja olivat Beenz, Flooz ja DigiCash, mutta kaikki yritykset epäonnistuivat digitaalisen valuutan luomisessa. Syypää tähän ei ollut teknologia itsessään, vaan yrityksien sisällä oli petoksia ja paljon taloudellisia ongelmia. Jokainen edellä mainituista valuutoista käytti kolmannen osapuolen lähestymistapaa, mikä merkitsi sitä, että niiden takana olevat yritykset tarkastivat ja helpottivat liiketoimia. Näiden yrityksien epäonnistumisen vuoksi digitaalisen kassajärjestelmän luominen pidettiin pitkään kadonneena. (Cointelegraph 2017).

Vuonna 2009 täysin anonyymi henkilö tai taho, joka tunnetaan nimellä Satoshi Nakamoto, esitteli Bitcoinin. Satoshi kuvaili sitä ”vertaisverkkoiseksi sähköiseksi kassajärjestelmäksi”. Se on täysin hajautettu, eli siihen ei ole palvelimia eikä se ole keskushallinnon valvontaviranomaisten valvonnassa. Konsepti muistuttaa läheisesti vertaisverkkoja tiedostojen jakamista varten. Yksi tärkeimmistä ongelmista, joita maksujärjestelmän on ratkaistava, on kaksinkertainen meno. Se on vilpillinen tekniikka, joka käyttää samaa summaa kahdesti. Perinteinen ratkaisu oli luotettava kolmas osapuoli, joka piti kirjaa saldoista ja liiketoimista. Nämä menetelmät edellyttivät kuitenkin aina sitä, että viranomaiset hallitsivat varoja ja kaikkia henkilökohtaisia tietoja. Hajautetussa verkossa, kuten Bitcoin ja Ethereum, jokainen osallistuja tekee tämän tehtävän yhdessä. Tämä tapahtuu lohkoketjun julkisen kirjanpidon kautta kaikista tapahtumista, jotka ovat tapahtuneet verkossa. Kaikki verkossa tapahtuneet tapahtumat ovat julkisia, joten käyttäjät voivat nähdä jokaisen tilin varat.

Jokainen transaktio on tiedosto, joka koostuu lähettäjän ja vastaanottajan julkisista avaimista. Transaktiolle täytyy saada myös lähettäjän yksityisen avaimen allekirjoitus. Kaikki tämä on vain osa perustason salausta, lopulta tapahtuma lähetetään verkossa eteenpäin, kun se on vahvistettu, kryptovaluutan verkon sisällä vain louhijat voivat vahvistaa tapahtumia ratkaisemalla kryptografisen ”palapelin”. Louhijat ottavat transaktion, tarkistavat sen aitouden, jonka jälkeen se levitetään verkolle. Tämän jälkeen jokainen verkon solmu lisää sen tietokantaa. Kun kauppa on vahvistettu, se muuttuu peruuttamattomaksi ja louhija saa palkkion sekä tapahtumamaksut transaktion käsittelystä. Pohjimmiltaan mikä tahansa kryptovaluutta perustuu kaikkien osallistujien yhteisymmärrykseen varojen ja tapahtumien aitoudesta. Verkkoon on rakennettu ja ohjelmoitu paljon sääntöjä, jotka estävät sen hajoamisen.

3 ETHEREUM

Yleisö kuuli ensimmäisen kerran lohkoketjutekniikasta, kun Bitcoin luotiin ja siitä kirjoitetut uutiset ja otsikot valtasivat erilaiset mediat ja uutislähteet. Bitcoin, hajautettu digitaalinen valuutta, antaa ihmisille mahdollisuuden lähettää ja vastaanottaa varoja toisilleen ilman tarvetta kolmannelle osapuolelle, kuten pankki- tai maksunvälitysjärjestelmää.

Lohkoketjuteknologia mahdollistaa vertaisverkon tapahtumien turvallisen ja laadukkaan suorittamisen ja helpottaa verkon kaikkia Bitcoin-siirtojen julkista kirjanpitoa ja valvoo saldoja. Lohkoketjuteknologia estää P2P-iskujen tapahtumisen, kuten kaksinkertaiset menot ja muut vilpilliset toiminnot. Vertaisverkkojen luontainen läpinäkyvyys ja kyky turvallisesti poistaa kolmas osapuoli digitaalisten maksutapahtumien siirroissa johtaa siihen, että kryptovaluuttoja voidaan käyttää todella monipuolisesti. Ethereumin ja Bitcoinin yhtäläisyydet ovat, että molemmat käyttävät lohkoketjuteknologiaa ja molemmat ovat kryptovaluuttoja, joita voidaan ostaa, myydä tai tuottaa louhimalla. Ohjelmoitava lohkoketju sekö avoimen lähdekoodin Ethereum-alustalla voi olla lukuisia käyttäjien luomia hajautettuja sovelluksia (DAPPS).

Käytännössä tämä tarkoittaa sitä, että ohjelmoijat voivat käyttää Ethereumia oman kryptovaluuttansa suunnitteluun ja toteuttamiseen, sekä tallettaa ja toteuttaa tulevia sopimuksia tai kauppoja, kuten kiinteistövälitystapahtumia tai testamentteja.

Kuten jokaisessa lohkoketjussa, jokainen verkkoon ohjelmoitu **s**olmu päivittää Ethereumin tietokantaa jatkuvasti. Ethereum Virtual Machine (EVM) voi suorittaa sovelluksia, jotka on ohjelmoitu suosituimmilla ohjelmointikielillä kuten JavaScript ja Python, joissa jokainen solmu suorittaa samat koodatut ohjeet.

EVM:n kaikki tietojenkäsittely suoritetaan rinnakkain koko verkossa, tuloksena on hajautettu yhteisymmärrys, joka takaa sen, että lohkoketju ei voi kaatua. Vikatiloissa ja katastrofien sattuessa palautuminen normaaliin toimintaan tapahtuu välittömästi ilman viiveitä. Kaikki tieto, joka on tallennettu Ethereumin lohkoketjuun, pysyy turvassa ja sen hakkerointi sekä manipulointi on mahdotonta. (Orgera 2018).

Ethereum-säätiön tehtävänä on tukea ja edistää alustan perustason tutkimustyötä, kehittämistä ja koulutusta, jotta hajautetut protokollat ja työkalut saadaan käyttöön ympäri maailmaa, mikä antaa sovelluskehittäjille mahdollisuuden tuottaa seuraavan sukupolven hajautettuja sovelluksia ja rakentaa yhdessä maailmanlaajuisesti saatavilla oleva, ilmainen ja luotettavampi internet.

Ethereum lainaa monia ominaisuuksia, joita on kokeiltu ja testattu monia vuosia vanhemmissa kryptovaluutoissa, kuten Bitcoinissa. Tästä huolimatta Ethereum eroaa huomattavasti tavasta käsitellä tiettyjä protokollaominaisuuksia ja myös monia tilanteita, jotka ovat pakottaneet Ethereumia kehittämään täysin uusia taloudellisia lähestymistapoja, koska se tarjoaa toiminallisuuksia, joita ei ole olemassa muilla järjestelmillä. Tarkoituksena on eritellä tärkeimmät ja suurimmat päätökset, joita tehtiin Ethereum-pöytäkirjan rakentamisprosessissa.

Kerrosrakenne: Kehittäjät halusivat Ethereumin pohjatason arkkitehtuurin olevan mahdollisimman yksinkertainen, jotta Ethereumin rajapinnat, mukaan lukien kehittäjien korkeatasoiset ohjelmointikielet ja käyttöliittymät pitäisi olla mahdollisimman helppo ymmärtää. Koska monimutkaiset ratkaisut ovat väistämättömiä, ne sijoitetaan pöytäkirjan keskimmäiseen kerrokseen, jotta loppukäyttäjät eivät näe niitä.

Vapaus: Käyttäjiä ei pidä rajoittaa mihin tai miten he käyttävät Ethereum-protokollaa, eikä tiettyjen sopimuksien tai liiketoimien suosiminen ole suotavaa.

Yleistyminen: Protokollan ominaisuuksissa ja op-koodeissa tulisi olla mahdollisimman alhaisen tason käsitteitä, jotta ne voidaan yhdistää, mukaan lukien tavat, jotka eivät välttämättä ole hyödyllisiä nykyään mutta saattavat tulla käyttökelpoisiksi myöhemmässä vaiheessa.

Ominaisuuksien puuttuminen: Yleistymisen seurauksena kehittäjät ovat kieltäytyneet rakentamasta jopa hyvin yleisiä korkean tason tapauksia protokollan sisäisiksi osiksi, sillä jos loppukäyttäjät todella haluavat tehdä sen, heillä on aina mahdollisuus luoda aliprotokollia esim. Bitcoin -> Litecoin. Esimerkkinä tästä on

Bitcoinin kaltaisen ”locktime”-ominaisuuden puuttuminen Ethereumista. ”Loctime” –ominaisuudella tarkoitetaan sitä osaa tapahtumasta, joka ilmaisee aikaisimman lohkon, milloin tapahtuma voidaan lisätä lohkoketjuun. Tällainen ominaisuus voidaan simuloida protokollan avulla, jossa käyttäjät lähettävät allekirjoitettuja datapaketteja. Nämä datapaketit voidaan syöttää erikoituneeseen sopimukseen, joka käsittelee ja suorittaa jonkin vastaavan toiminnon, jos datapaketti on tietyssä sopimuskohtaisessa mielessä pätevä.

Riskiaversion puuttuminen: Ethereumin kehittäjät ovat hyväksyneet korkeamman riskitason, koska se tarjoaa erittäin merkittäviä etuja. Etuja ovat esimerkiksi:
- yleistetyt tilasiirtymät,
- 50 kertaa nopeammat lohkoajat (Bitcoinin lohkoaika on 10 minuutta ja Ethereumin 20 sekuntia) (Github 2017).

4 LOHKOKETJU

Lohkoketju muodostuu lohkosta sekä ketjusta. Lohko kaiken verkon sisällä tapahtuvan datan, esimerkiksi yksittäisen transaktion, jossa Ethereumia siirretään pörssistä lompakkoon. Ketjulla tarkoitetaan verkon rakennetta, jossa jokainen uusi lohko lisätään aiempien jatkoksi ja tätä kokonaisuutta kutsutaan lohkoketjuksi. Tiedonsiirrosta lohkoketjussa vastaavat solmut, jotka päivittävät kaiken verkossa tapahtuvan tiedon julkiseen tilikirjaan.

Lohkoketju on nimensä mukaisesti hajautettu tietojärjestelmä, joka koostuu lohkoista. Jokainen lohko sisältää suuren määrän tietoa jokaisesta lohkoketjussa tapahtuvasta transaktiosta.

1. Lohkot tallettavat seuraavat tiedot transaktiosta, päivämäärän, ajan ja transaktion arvon.
2. Lohkoihin tallentuu myös tieto siitä ketkä ovat osallisena transaktiossa, sen sijaan että käytettäisiin todellisia nimiä, ostoksesi tallennetaan ilman yksilöiviä tietoja käyttämällä ainutlaatuista ”digitaalista allekirjoitusta”, joka on ikään kuin käyttäjätunnus.
3. Jokaisella lohkolla on oma ns. DNA, tätä tietoa kutsutaan nimellä ”hash” ja se erottaa lohkot toisistaan. Jos lohkoon tallentuisi esimerkiksi kaksi täysin identtistä transaktiota, joissa vastaanottaja, lähettäjä ja transaktion arvo olisivat täysin identtiset, voitaisiin nämä kaksi transaktiota erottaa toisistaan ainutlaatuisen hash koodin avulla.

Yllä oleva on vain karkea esimerkki siitä, mitä lohkoketjun sisällä tapahtuu, todellisuus on hieman erilainen. Yksittäinen lohko lohkoketjussa voi tallentaa suuren määrän dataa, transaktioiden koosta riippuen yhteen lohkoon mahtuu tuhansia tapahtumia.

Kuva 1. Lohkoketjun toimintaperiaate (Rissanen 2016).

Kuvassa 1 On kuvattu rahansiirtoa henkilöiden välillä lohkoketjua käyttäen.

4.1 Louhinta

Louhijoilla on todella tärkeä tehtävä varmistaa, että Ethereum-verkko toimii. Monet uudet käyttäjät ajattelevat, että louhinnan ainoa tarkoitus on luoda eettereitä tavalla, joka ei vaadi vaan kaupankäyntiä. Tämä on osittain totta, Ethereumin rahakkeet luodaan louhinnan avulla 2-3 eetterin nopeudella louhittua lohkoa myöten.

Louhinnalla on kuitenkin toinen vielä tärkeämpi rooli, joka on tapahtumien aitouden tarkistaminen ja mahdollisten väärinkäyttöjen estäminen, joka on normaalisti pankkien tehtävä. Louhijat varmistavat, että käyttäjät toimivat rehellisesti ja ettei rahoja käytetä useammin kuin kerran. Lohkoketju luo täysin uudenlaisen tietojenkäsittelytavan, jossa koko verkko tarkistaa tapahtumien aitouden, jonka jälkeen ne kirjataan julkiseen tilikirjaan. Louhinta mahdollistaa hajautetun kirjanpidon. Verkon louhijat pääsevät yksimielisyyteen tapahtumahistoriasta ja petosten estämisestä. Tämä oli yleinen ongelma, jota ei aiemmin osattu ratkaista ennen hajautettujen kryptovaluuttojen syntymistä.

Nykyisin Ethereumin louhintaprosessi on täysin samanlainen kuin Bitcoinin. Yksinkertaistettuna louhijat käyttävät tietokoneidensa laskentatehoa arvatakseen vastauksia lohkoketjun palapeliin, kunnes yksi louhija saa vastauksen oikein ja hänet

palkitaan. Sama prosessi toistuu jokaisen lohkon kohdalla, kunnes joku selvittää vastauksen, jonka jälkeen sama prosessi alkaa seuraavassa lohkossa. Mitä enemmän laskentatehoa tietokoneesta löytyy, sitä todennäköisemmin se löytää vastauksen lohkon matemaattiseen palapeliin. Jos louhija löytää hashin (lohkon sisältämästä datasta laskettava tiiviste) joka vastaa nykyistä louhittavaa kohdetta, louhijalle myönnetään lohkon sisältämät eetterit palkinnoksi. Tieto tapahtuneesta kulkeutuu lohkoketjua pitkin verkon jokaiselle solmulle, jotka päivittävät tiedon verkon julkiseen tilikirjaan. Verkon louhijat löytävät uuden lohkon noin 14 sekunnin välein, jos lohkojen palapelien ratkaisemiseen kuluva aika nopeutuu tai hidastuu huomattavasti, verkon algoritmi säätää pulmien vaikeustasoa automaattisesti, jotta siihen kuluva aika palautuu noin 14 sekuntiin. (Frankenfield 2018; Hertig 2017).

4.2 Avoin lähdekoodi

Projektit, tuotteet tai aloitteet kattavat avoimen vaihdon. Ethereumin lohkoketjun toimintaperiaate ja koodaus on tehty julkisesti nähtäväksi, jolloin jokainen käyttäjä voi halutessaan tutustua Ethereumin toimintatapaan, sekä muokata ja käyttää sitä haluamallaan tavalla omaan käyttöönsä. Avoimella lähdekoodilla saadaan myös luotettavuutta aikaiseksi, jolloin se on ns. läpinäkyvä eikä koodiin kätketty mitään mistä käyttäjät eivät tietäisi.

Avoimen lähdekoodin ohjelmistojen osalta koodi on vapaasti ladattavissa ja muunneltavissa vapaasti, kunhan käyttäjä noudattaa mitä ohjelmistolisenssisopimuksessa on sovittu. Avoimen lähdekoodin ohjelmisto on yleensä julkisen lisenssin (GNU) alla, mutta on olemassa myös muita lisenssejä. (Opensource).

4.3 Älykkäät sopimukset

Älykkäät sopimukset ovat lohkoketjuun ohjelmoituja koodilohkoja, jotka voivat itse suorittaa tiettyjä toimintoja tietyillä parametreillä, kun ennalta määrittyvät kriteerit täyttyvät. Älykkäät sopimukset aktivoituvat, kun joku lähettää tapahtuman lohkoketjussa, joka täyttää sopimuksen ennalta määritellyt kriteerit. Helpoin tapa havainnollistaa älykäs sopimus on sen vertaaminen juoma-automaattiin:

1. Syötät rahaa juoma-automaattiin.
2. Seuraavaksi automaatti tunnistaa, mikä kolikoiden yhteisarvo on.
3. Valitset tuotteen ja kone pudottaa valitsemasi tuotteen kaukaloon, josta käyttäjä nostaa sen.
4. Jos syötit automaatille liikaa rahaa, se palauttaa ylimääräiset kolikot.

Myyntiautomaatti on todella vanha keksintö eikä sen tekniikassa ei ole mitään erikoista, mutta sen toimintaperiaate on todella varma ja sopimukset tapahtuvat aina samalla tavalla, sama pätee älykkäisiin sopimuksiin.

Älykkäiden sopimuksien käyttäminen yleistyy monilla aloilla, joista loistava esimerkki on kiinteistövälitys. Tavallisesti kiinteistövälityksessä kuten asunnon myymisessä on huomattavasti kuluja ja maksuja, kuten välittäjälle maksettavat palkkiot, markkinointikulut ja mahdolliset käsittelymaksut ja varainsiirrosta aiheutuvia kuluja. Asunnon myyminen älykkään sopimuksen avulla säästää huomattavan summan rahaa ja aikaa, koska sopimuksen avulla määrität ennakkoon lohkoketjuun tietyt parametrit ja kun sopiva ostaja on löytynyt, joka täyttää kriteerit, sopimus täyttyy automaattisesti silmän räpäyksessä ja sopimus tallentuu lohkoketjuun. (Blockgeeks 2017).

Kuva 2. Lohkoketjun edut yritykselle (Rubygarage 2018).

Kuvassa 2 on eritelty muutamia älykkäiden sopimuksien tuomia ominaisuuksia perinteisiin sopimuksiin verrattuna esim. Pienemmät kulut, julkinen tilikirja, petoksien minimaalinen riski sekä suora kahden käyttäjän välinen sopimus ilman kolmatta osapuolta.

4.4 Älykkäiden sopimuksien edut

Älykkäät sopimukset ovat autonomisia, itsenäisiä sopimuksia. Nämä virtuaaliset sopimukset voivat helpottaa esimerkiksi rahan, sisällön, osakkeiden tai arvon vaihtoa. Näiden sopimuksien itsensä toteuttava luonne tarjoaa monia mahdollisuuksia käyttää niitä alasta riippumatta.

Älykkäiden sopimuksien tuomia etuja ovat:

1. Autonomia – Käyttäjä on itse vastuussa sopimuksen tekemisestä ja siitä millaisilla ehdoilla sopimus täyttyy, jolloin kiinteistövälittäjän tai asianajajan palvelut eivät ole enää tarpeellisia. Koska sopimuksissa ei ole kolmatta osapuolta, sopimuksia on mahdoton peukaloida tai virheiden sattumista ei tarvitse pelätä laisinkaan, sen sijaan että sopimusta hoitaisi useampi taho ja kymmenet ihmiset.
2. Luottamus ja turvallisuus– Asiakirjat salataan jaettuun julkiseen tilikirjaan, joten niiden kadottaminen tai hakkeroiminen on käytännössä mahdotonta.
3. Nopeus – Asiakirjojen manuaalinen käsittely vaatii paljon aikaa, sekä paperitöitä. Älykkäät sopimukset käyttävät ohjelmistokoodia tehtävien automatisoimiseksi, joka säästää huomattavasti aikaa ja rahaa.

4. Tarkkuus – Automatisoidut sopimukset eivät ole pelkästään nopeampia ja halvempia, vaan myös välttävät kaikenlaisia virheitä, joita saattaa esiintyä lomakkeiden manuaalisesta täyttämisestä.
5. Paperittomuus – Yhä useammat yrityksen eri puolilla maailmaa ovat tietoisempia ympäristövaikutuksistaan. Älykkäät sopimukset mahdollistavat ”vihreän” liikkeen, koska ne toimivat täysin virtuaalimaailmassa, joten tämä poistaa tarpeen käyttää paperia.
6. Kulut – Älykkäiden sopimuksien yksi merkittävimmistä eduista on se, että ne eliminoivat laajan välittäjäketjun tarpeen, johon kuuluu esim. lakimiehet, todistajat, pankit sekä välittäjät.

Tyypillisiä käyttökohteita ovat syntymä- ja kuolintodistukset, omistusasiakirjat, rahoitustilit, lääketieteelliset todistukset sekä kauppakirjat ja kaikki muut, jotka voidaan tallentaa tietokoneen koodiin. Ethereumia pidetään sopimuksien tulevana teknologiana ainutlaatuisen lohkoketjunsa ansiosta. (Blockgeeks 2017, Medium 2017).

Kuva 3. Perinteinen sopimus vs Älykäs sopimus (Davies 2017).

Kuvassa 3 Verrataan perinteisien sopimuksien (vasen) ja älykkäiden sopimuksien (oikea) eroja. Älykkäiden sopimuksien parhaimmat ominaisuudet verrattuna perinteisiin sopimuksiin ovat nopeus, minimaaliset kulut, mahdoton väärentää ja kolmansien osapuolien tarpeettomuus.

4.5 Transaktiot

Ethereumin lohkoketjun yksittäiset kaupat eli transaktiot ovat peruskäyttäjälle nopea tapa siirtää valuuttaa lompakosta toiseen, mutta se mitä lohkoketjussa todella tapahtuu, on monen eri tapahtuman ketju. Transaktio on tapa, jolla ulkoinen maailma on vuorovaikutuksessa Ethereum-verkon kanssa. Transaktiota käytetään, kun halutaan muokata tai päivittää Ethereum-verkkoon tallennettua tietoa.

Ethereum on tilipohjainen lohkoketjulla toteutettu kryptovaluutta. Tilejä on kahdentyyppisiä: Ulkoisesti omistettuja tilejä sekä Sopimustilejä, seuraavaksi pyrin avaamaan molemmat tilityypit mahdollisimman loogisesti. (Murthy 2017).

4.6 Ulkoisesti Omistetut Tilit (UOT)

Ulkoisesti omistettuja tilejä voidaan kuvailla ikään kuin yksittäisinä käyttäjinä ulkoisessa maailmassa. Ethereum-verkon käyttäjää edustaa 20-tavuinen ja 160 bittinen osoite. Ethereum-verkon sisällä kiertää sen natiivi valuutta: eetteri. Alkuperäisen valuutan lisäksi eetteriä käytetään pääasiassa transaktiomaksuna tai palvelumaksuna, jota kutsutaan nimellä Gas (kaasu), kun Ethereum-verkko käsittelee tapahtumaa. Jokaisella ulkoisesti omistetulla tilillä on oma varattu tila eetterinä ja kun UOT aloittaa transaktion, kaasun määrä määritellään joka transaktioon ja mitä enemmän kaasua transaktiossa käytetään, sitä nopeammin se toteutuu.

Sopimukset Ethereum-verkossa ovat ns. älykkäitä sopimuksia, joilla liiketoimintalogiikka toteutetaan. Sopimukset luodaan ensiksi ihmisille luettavalla koodikielellä

nimeltä Solidity, tämän jälkeen se muutetaan koneellisesti ymmärrettäväksi koodiksi nimeltä bytecode (bittikoodi), jota käytetään Ethereum-verkossa.

Sopimukseen ohjelmoidaan toimintoja, jotka määrittelevät todellisen liiketoimintalogiikan, ja toimintoja kutsutaan vain kerran, kun sopimus laitetaan käytäntöön ja näin ollen sopimuksia ei pysty tekemään useaan kertaan. (Murthy 2017, Tam 2018).

4.7 Sopimustili

Aiemmin mainittu tavukoodi ei ole käytettävissä ennen kuin se on sijoitettu Ethereum-verkkoon. Sopimuksen bittikoodin käyttöönotto tapahtuu transaktion kautta. Sopimustili luodaan käytetyn sopimuksen mukaisesti.

Sopimustilit tunnistetaan uniikilla sopimusosoitteella, joka on myös 20-tavuinen osoite. Tämä on osoite, jota käytetään kuten minkä tahansa UOT: n tilin kanssa, sopimustili voi myös säilyttää eetterit, mikäli ne sopivat liiketoimintalogiikkaan. (Murthy 2017).

4.8 Transaktion rakenne

Vaikka Ethereumin transaktioita voi käyttää useaan eri tarkoitukseen, sen rakenne on aina samanlainen.

Transaktioita on kolmea eri tyyppiä:

1. Varojen siirto kahden UOT: n välillä.
2. Älykkään sopimuksen luominen Ethereum-verkossa.
3. Tehtävän suorittaminen käyttöönotetussa älykkäässä sopimuksessa.

Alla oleva transaktio on suoritettu Go Ethereum Client (GETH) ohjelmalla. Sovelluksella pystytään suorittamaan useita toimintoja Ethereum-verkossa, kuten siirtämään varoja tilien välillä, tarkastelemaan lohkojen tapahtumia sekä luomaan sopimuksia.

Keneltä: Transaktion lähettäjä, joka on tunnistettavissa 20-tavuisesta osoitteesta.

Kenelle: Transaktion vastaanottaja, joka on myös tunnistettavissa 20-tavuisella osoitteella ja riippuen käyttötarkoituksesta vastaanottaja voi olla Sopimustili tai Ulkoisesti Omistettu Tili.

Arvo: Transaktion arvon määrä eettereissä. Jos transaktion vastaanottaja on Ulkoisesti Omistettu Tili, niin kyseessä on varojen siirto, mutta jos vastaanottaja on tyypiltään Sopimus Tili niin transaktion tarkoitus ja arvo on määritelty ennakkoon sopimuksessa.

Sisältö / Data: Tämä kenttä on tarkoitettu pääasiassa sopimuksiin liittyviin asioihin. Sopimusfunktion suorittamiseksi se sisältää allekirjoituksen ja koodatut argumentit. Tämä kenttä jätetään tyhjäksi rahansiirrossa.

Kaasun hinta ja Kaasun Raja: Molemmat ovat tärkeä osa transaktion kustannusten käsittelyyn. Kaikkien verkossa toimivien louhijoiden suorittamille tehtäville on ennalta määritellyt kustannukset. Transaktion suorittamiseen tarvittava määrä ei ylitä ennalta asetettua kaasurajoitusta, jos tapahtuman käsittelyssä ilmenee poikkeuksia tai ongelmia.

Tapahtuman allekirjoittaminen: Esimerkki transaktiossa käytettiin GETH: iä, joten sovellus hoitaa tapahtuman allekirjoittamisen ”puolestani”. Allekirjoittaminen on prosessi, jossa siihen luodaan uniikki allekirjoitus käyttäen tapahtuman lähettäjän yksityistä avainta. Allekirjoitettu transaktio käsitellään yllä olevien vaiheiden kanssa, kunnes allekirjoitettu tapahtuma kirjataan lohkoketjussa seuraavaksi syntyvään uuteen lohkoon. (Murthy 2017, Tam 2018).

5 HAJAUTETUT SOVELLUKSET

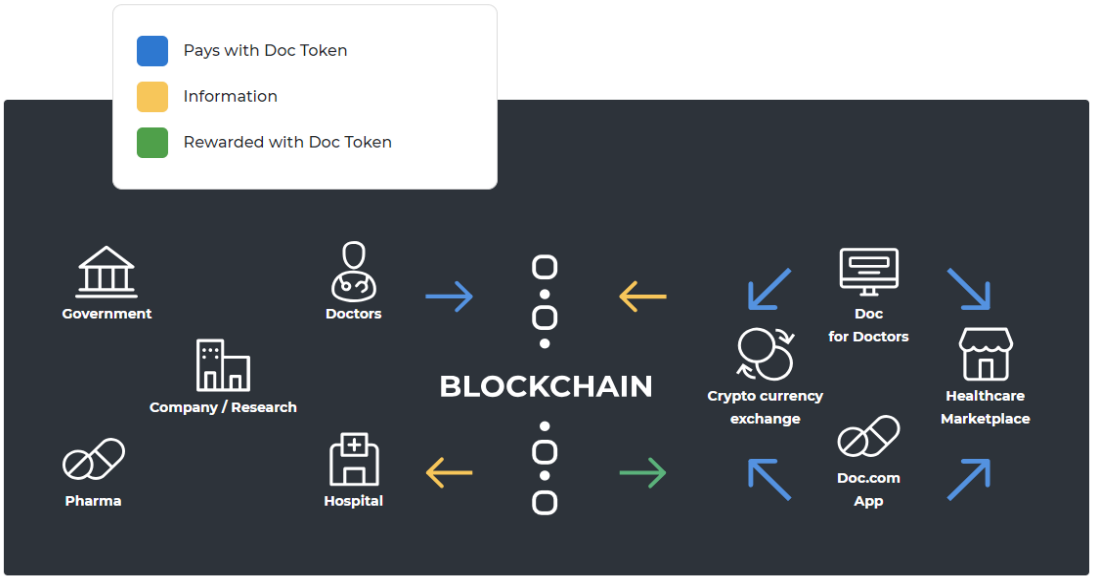
Maailmassa on satoja tuhansia sovelluksien kehittäjiä, jotka ovat rakentamassa seuraavan sukupolven hajautettuja sovelluksia (DAPP) Ethereumin maailmanlaajuisesti hajautetun lohkoketjun päälle. Vaikka lohkoketjun avulla kehitettävien ekosysteemien rakentaminen vie paljon aikaa, on olemassa monia tahoja, jotka ovat kehittäneet toimivia sovelluksia ja yrityksiä Ethereumin lohkoketjun päälle.

Tämä hajautettujen sovelluksien aalto kehittyy useilla markkinoilla hurjaa vauhtia ja niiden käyttö yleistyy useilla maailmanlaajuisilla markkinoilla. Lohkoketjun yleistyminen maailmalla ajaa yrityksiä kohti uutta aikakautta, jossa spekuloinnille ja virheille ei ole tilaa.

Seuraavaksi kerron muutamasta Ethereumin päälle rakennetuista hajautetuista sovelluksista, jotka ovat jokapäiväisessä käytössä ja saatavilla ilmaiseksi ympäri maailman, joko matkapuhelimien sovelluskaupoista tai suoraan yrityksien verkkosivujen kautta.

Doc.com

DocHealth on ainoa markkinoilla oleva sovellus, joka tarjoaa asiakkaalle ilmaisen lääketieteellisen tuen 24 tuntia vuorokaudessa videopuhelun avulla. Mobiilisovelluksen avulla saat suoran videoyhteyden lääketieteen ammattilaisiin, jotka pyrkivät auttamaan parhaansa mukaan aina mahdollisimman nopeasti. Yhtiöllä on myös toinen sovellus nimeltä DocEmotions, jonka toimintaperiaate on samanlainen, mutta sovelluksen avulla luodaan videoyhteys mielenterveyden ammattilaiselle. Sovelluksen käyttäjien tiedot tallennetaan Ethereumin lohkoketjuun, jossa tiedot pysyvät turvassa eikä niitä voida käyttää väärin. Palvelua käyttävät asiakkaat saavat antamistaan potilastiedoista palkinnoksi Doc-rahakkeita, joilla on rahallista arvoa ja ne voidaan myydä pörssissä. (Coindigital 2018).



Kuva 4. Doc.com toimintaperiaate.

Kuvassa 4 on selvitetty Doc.comin tarjoaman sovelluksen toimintaperiaate, jossa nuolet kuvaavat tiedon (oranssi) ja palkkioiden (vihreä) siirtymisen sovelluksen ja asiakkaan välillä. Siniset nuolet kuvaavat, miten palkkio jakautuu lääkärien, palvelun ja pörssien välillä.

Golem

Golem tarjoaa alustan, jonka kautta voidaan hyödyntää muiden verkossa olevien tietokoneiden laskentatehoa. Yrityksen tarjoama palvelu on ikään kuin hajautettu supertietokone, josta voidaan tarvittaessa ostaa laskentatehoa tai päinvastoin myydä tietokoneesi laskentatehoa muiden käyttöön. Verkossa laskentatehoa vuokraavat käyttäjät palkitaan GNT-rahakkeilla, joita voidaan käyttämään palvelun sisällä tai myymään FIAT valuutoiksi useissa pörsseissä.

Ethereumin verkkoon on rakennettu useita mielenkiintoisia sovelluksia, mutta suuri haittapuoli niiden käyttöönotossa on korkeat kaasumaksut. Kun verkko on ruuhkainen, liiketoiminta voi olla hidasta ja kaasumaksut kalliita. Ethereumin kehittäjät ovat tietoisia tästä ongelmasta ja ovatkin jo aloittaneet verkon skaalaamisen, jotta sen toimivuus paranee entisestään ja maksut pysyvät mahdollisimman pieninä. (Gutteridge 2018).

6 ETHEREUMIN OSTO JA MYYNTI

Ethereumin hankintaan on useita vaihtoehtoja, sitä voidaan ostaa sitä suoraan FIAT valuutoilla kuten euroilla sekä dollareilla ja siihen tarvitset ainoastaan pankki- tai luottokortin tai vaihtoehtoisesti pankkitilin, jolla kansainvälisten siirtojen tekeminen on helppoa. Kryptovaluuttojen ostaminen nykyään on huomattavasti helpompaa kuin muutama vuosi sitten, jolloin käyttäjien täytyi ostaa ensiksi Bitcoinia, jonka jälkeen se oli muutettava Ethereumiksi pörssissä ja vasta sen jälkeen sen pystyi siirtämään omaan lompakkoon. Nykyisit käyttäjät voivat ostaa ja säilyttää Ethereumin pörssissä, joka säästää huomattavasti aikaa, sekä käsittelykuluista syntyviä kuluja. Seuraavaksi suosittelen muutamaa välittäjää, joista voit ostaa Ethereumin lisäksi useita muita kryptovaluuttoja ja mainitsen jokaisen välittäjän hyvät ja huonot puolet.

Coinbase

Coinbase on maailman suosituin ja tunnetuin pörssi, koska sivusto mahdollistaa luottokortilla ostamisen. Coinbase tarjoaa myös muiden kryptovaluuttojen ostamisen kuten Bitcoinin, Litecoinin ja Bitcoin Cashin.

Hyvää – Helppokäyttöinen, Hyväksyy luottokorttiostamisen.

Huonoa – Hidas asiakaspalvelu, korkeat osto kulut ja kryptovaluuttojen suppea tarjonta.

Poloniex

Poloniex on yksi vanhimmista sivustoista kryptovaluuttojen ostamiseen ja sivustolla on mahdollista ostaa yli 60 eri kryptovaluuttaa. Järjestelmä tarjoaa syvällistä tietoa kryptovaluutoista ja siihen liittyvistä asioista sekä laajan valikoiman hyödyllisiä työkaluja kolikoiden analysointiin.

Hyvää – Laaja valikoima kryptovaluuttoja ja hyvät työkalut.

Huonoa – Sekä verkkosivu että asiakaspalvelu ovat hitaita. (Sebfor 2017).

Binance

Binance jakaa paikan maailman suosituimpana pörssinä Coinbasen kanssa. Maltalla toimiva pörssi on saavuttanut suosionsa todella matalien kulujensa ansiosta, todella suuresta valikoimasta kryptovaluuttoja sekä verkkosivut on käännetty monelle kielelle. Binancen tarjoamalla palvelulla on suurin päivittäinen vaihto kaikista pörsseistä.

Hyvää – Alhaiset kaupankäyntikulut, hyvä sovellus sekä tietokoneelle, että puhelimelle. Todella suuri valikoima kryptovaluuttoja sekä suuri päivittäinen vaihto.

Huonoa – Ei huonoja puolia. (Dob 2019).

7 ETHEREUMIN SÄILYTTÄMINEN

Kun ensimmäiset kryptovaluutat on hankittu, seuraavaksi herää kysymys, missä niitä kannattaa säilyttää ja miksi. Kryptovaluuttojen säilyttämiseen on monta mahdollisuutta digitaalisesta lompakosta paperisäilytykseen. Tässä osiossa selvitetään yleisimmät vaihtoehdot Ethereumin säilyttämiseen ja jokaisen vaihtoehdon hyvät ja huonot puolet.

Paperilompakko

Paperilompakko on turvallisin tapa säilyttää Ethereumia. Paperilompakko toteutetaan siten, että paperille kirjoitetaan jokaisen kolikon yksityinen avain ns. kolikon oma DNA, jonka jälkeen paperi säilötään talletuslaatikkoon tai kassakaappiin. Paperilompakoiden käyttäminen on suositeltavaa pitkäaikaiselle sijoittajalle tai suuria määriä omistavalle.

Hyvää – Turvallisin tapa säilyttää Ethereumia.

Huonoa – Epäkäytännöllinen säännölliseen käyttämiseen.

Säilyttämiseen tarkoitetut (offline) laitteistot

Aivan kuten paperilompakot, kryptovaluuttojen säilyttämiseen suunnitellut laitteistot ovat myös erittäin turvallinen vaihtoehto. Yksinkertaistettuna laite on USB-tikun kaltainen kannettava laite, johon talletetaan kryptovaluuttojen yksityisiä avaimia, jonka jälkeen laitteen voi halutessaan sulkea, vaikka kassakaappiin. Laitteistot eivät ole yhteydessä internettiin, joten niitä ei voi kukaan ulkopuolinen myöskään hakkeroida. Esimerkiksi seuraavat laitteet on tarkoitettu kryptovaluuttojen säilyttämiseen: Ledger Nano S (69e) sekä Trezor Hadware Wallet (89e).

Hyvää – Erittäin turvallinen vaihtoehto ja tukee myös muita kryptovaluuttoja Ethereumin lisäksi.

Huonoa – Kaikki markkinoilta löytyvät laitteet ovat maksullisia.

Ethereum työpöytälompakot

Tietokoneelle ladattavat sovellukset ns. työpöytälompakot ovat toiseksi turvallisimpia vaihtoehtoja valuuttojen säilyttämiseen. Niiden suojaustasot ovat todella korkeat, mutta suosittelen hankkimaan erittäin hyvän virustorjuntaohjelman sekä palomuurin ennen suurien summien tallettamista tietokoneellesi.

Esim. Coinbase Wallet lompakkoon voit tallentaa mm Ethereumia, Bitcoinia ja Litecoinia. Coinbase Wallet tarjoaa myös kaksivaiheisen vahvistuksen sekä muita palveluita.

Hyvää – Tukee monia kryptovaluuttoja, hyväksyy luottokortteja, helppokäyttöinen sekä sovelluksesta löytyy mobiilisovellus.

Huonoa – Hidas asiakaspalvelu, Tietokoneen hakkeroinnin riski ja virukset.

Näillä työkaluilla päästään jo hyvin alkuun, aina kannattaa kuitenkin itse tutkia ja vertailla saatavilla olevia palveluita ja laitteita, koska kaikilla on omat puolensa ja haluat varmasti löytää sen parhaimman vaihtoehdon. (Sebfor 2017, Velu 2017).

8 YHTEENVETO

Opinnäytetyöni tarkoitus oli tehdä opas sijoittajille, joille Ethereum ei ole ennestään tuttu. Sijoittajat, jotka lukevat tämän opinnäytetyön saisivat selvän käsityksen siitä, mitä Ethereum on, mitä käyttötarkoituksia sillä on ja mistä sitä hankitaan sekä missä sitä säilytetään turvallisesti. Onnistuin mielestäni vastaamaan näihin kysymyksiin hyvin ja esittämään kappaleet yksinkertaisesti, menemättä liian syvälle Ethereumin tekniikkaan, jotta sijoittajat, jolla ei ole kokemusta kryptovaluutoista pystyisivät sisäistämään lukemaansa tekstiä.

Ethereum oli minulle entuudestaan tuttu, koska olen seurannut kryptovaluuttojen kehitystä sekä markkinoita jo useamman vuoden ajan, mutta opinnäytetyötä tehdessäni opin paljon uusia asioita Ethereumin toiminnasta ja lohkoketjuista.

On selvää, että tulevaisuudessa Ethereum on tärkeä osa yrityksien arkea, koska sen tuomat edut sekä sovelluksien kehityksessä, että älykkäiden sopimuksien tarjoamat edut ovat todella merkittävät. Lähivuosien aikana näemme kuinka yhä useammat suuryritykset hyödyntävät lohkoketjuteknologian tuomia etuja ja mahdollisuuksia.

LÄHTEET

Blockgeeks. 2017. Smart Contracts. Viitattu 22.10.2018. https://blockgeeks.com/guides/smart-contracts/

Blockgeeks. 2017. What Is Ethereum? Viitattu 15.3.2019. https://blockgeeks.com/guides/ethereum/

ChainTrade. 2017. 10 Advantages of Using Smart Contracts. Viitattu 26.3.2019. https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a

Coindesk. 2017. What Are Cryptocurrencies, Guide for Beginners. Viitattu 2.2.2019. https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies#history

Coindigital, 2018. What is Docademic? https://www.coindigital.com/what-is-docademic-mtc/

Frankenfield, J. 2018. Block Time (Cryptocurrency). Viitattu 8.11.2018. https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp

GitHub. 2016. Design Rationale. Viitattu 18.1.2019. https://github.com/ethereum/wiki/wiki/Design-Rationale

Gutteridge, D. 2018. What is Golem? https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

Hertig, A. 2017. How Ethereum Mining Works. Viitattu 6.3.2019. https://www.coindesk.com/information/ethereum-mining-works/

Murthy. M. 2017. Life Cycle of an Ethereum Transaction. Viitattu 17.2.2019. https://medium.com/blockchannel/life-cycle-of-an-ethereum-transaction-e5c66bae0f6e

Opensource. 2015. What Is Open Source? Viitattu 22.1.2019. https://opensource.com/resources/what-open-source

Orgera, S. 2018. What Is Ethereum? Viitattu 14.3.2019. https://www.lifewire.com/what-is-ethereum-4154064

Sebfor. 2017. How to Buy & Store Ethereum – The Newbie Guide. Viitattu 14.2.2019. http://sebfor.com/how-to-buy-and-store-ethereum-securely-13/

Tam. K. 2018. Transactions in Ethereum. Viitattu 5.1.2019. https://medium.com/coinmonks/transactions-in-ethereum-e85a73068f74

Velu. S. 2017. How to Keep Your Cryptocurrency Safe: 7 Must Have Wallets. Viitattu 15.3.2019. https://blockgeeks.com/cryptocurrency-safe/