TAMPEREEN
AMMATTIKORKEAKOULU

Lohkoketjun rakenne ja kryptovaluutat

Miro Wallin

Opinnäytetyö
Joulukuu 2018
Tieto- ja viestintätekniikan koulutus
Ohjelmistotekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Ohjelmistotuotanto

WALLIN MIRO
Lohkoketjun rakenne ja kryptovaluutat

Opinnäytetyö 20 sivua
Joulukuu 2018

Tässä opinnäytetyössä käydään läpi avoimeen lähdekoodiin perustuvaa lohkoketjuteknologiaa. Lohkoketjulla toimivia kryptovaluuttoja on maailmassa satoja ellei tuhansia, mutta tässä työssä esimerkkinä käytetään niistä tunnetuinta eli Bitcoinia. Bitcoin on hyvin erilainen tapa perinteisiin tapoihin siirtää varallisuutta internetissä, koska se on täysin avoin, eikä transaktioihin tarvita lainkaan kolmannen osapuolen instituutioita.

Lohkoketjulla toimivat kryptovaluutat ovat täysin riippuvaisia käyttäjistä ja niiden ylläpitämästä vertaisverkosta ja siihen sisältyvistä salausalgoritmeistä. Opinnäytetyössä pilkotaan lohkoketjun rakenne pienempiin osiin ja kerrotaan eri komponenttien tehtävät lohkoketjussa ja käydään läpi millaisia vaiheita siirron tekemiseen ja validointiin liittyy. Lisäksi tässä selvityksessä kerrotaan esimerkkejä käyttökohteista, jossa lohkoketjuteknologiaa voidaan hyödyntää.

Asiasanat: kryptovaluutta, lohkoketju, Bitcoin

ABSTRACT

Tampere University of Applied Sciences
Information and communications technology
Software engineering

WALLIN MIRO
The structure of blockchain and cryptocurrencies

Bachelor's thesis 20 pages
December 2018

This bachelor’s thesis deals with open-source based technology. In the world, there are hundreds or thousands of cryptographic currencies working on blockchain, in this thesis Bitcoin is used as an example since it’s the most widely used cryptocurrency. Bitcoin is a very different way to the traditional systems to transfer assets on the internet, because it is fully open, and no third-party institutions are needed for transactions. Blockchain based currencies are completely dependent on users and their Peer-to-Peer network and the encryption algorithms involved.

In the thesis, the structure of the blockchain is fragmented into smaller parts and the steps of the components are explained. In addition, this report provides examples of applications where blockchain technology can be utilized.

Key words: blockchain, cryptocurrency, Bitcoin

SISÄLLYS

ERITYISSANASTO

algoritmi	Yksityiskohtainen kuvaus tai ohje siitä, miten tehtävä tai prosessi suoritetaan; jota seuraamalla voidaan ratkaista tietty ongelma.
escrow	Escrow on tili, jonka avulla pyritään pienentämään kaupallisiin transaktioihin liittyvää petoksen riskiä. Menettelyssä osapuoli voi tallettaa esimerkiksi maksun tai arvopaperin kolmannen luotetun osapuolen haltuun.
kryptovaluutta	Kryptografiaan perustuva digitaalinen virtuaalivaluutta.
transaktio	yksittäinen tehty vasteellinen kauppa, vaihto.
node	Lohkoketjun ylläpitoon osallistuva tietokone.
UTXO	Järjestelmä, joka määrittää Bitcoin-osoitteen balanssin.
lohkoketju	Useimpien kryptovaluuttojen pohjalla oleva tekniikka, jolla toisilleen vieraat toimijat voivat yhdessä tuottaa ja ylläpitää hajautettua lokia transaktioista.
kryptografia	Termi kryptografia on kreikankielistä alkuperää, sillä kreikan sana "kryptos" tarkoittaa salattua ja "graphos" tarkoittaa kreikankielessä kirjoitusta.
validoida	varmentaa, vahvistaa.

1 JOHDANTO

Sähköinen maksuliikenne ja maksujärjestelmät ovat perinteisesti luottaneet kolmansiin osapuoliin, kuten pankkeihin ja luottokorttiyhtiöihin varmistaakseen turvalliset transaktiot osapuolten välillä. Näiden järjestelmien käyttäjien on luotettava siihen, että kolmas osapuoli toimii instituutiona rehellisesti ehtojensa mukaisesti. Luottopohjaisia toimintoja on vaikea toteuttaa digitaalisessa järjestelmässä ilman sääntelyä ja jatkuvaa turvaamista. Teknologian kehitys on kuitenkin mahdollistanut täysin digitaaliset transaktiot ilman, että joudutaan luottamaan kolmanteen osapuoleen.

Lähivuosina markkinoille on ilmestynyt erilaisia virtuaali- tai vertaisvaluutoiksi kutsuttuja innovaatioita. Näitä digitaalisen ajan vaihdannan välineitä käytetään oikean valuutan tapaisesti, mutta toisin kuin perinteiset valuutat, kryptovaluutat ovat täysin sähköisiä, eikä niitä ole olemassa fyysisessä muodossa kuten kolikoina tai seteleinä. Kryptovaluutta teknologiaa voidaan hyödyntää monenlaisiin arvonsiirtoihin ja sopimuksiin kuten esimerkiksi normaaliin kaupankäyntiin tai etätyön ostamiseen. Kryptoteknologian avulla transaktio voidaan kohdistaa kenen tahansa kanssa, jolla on puhelin tai päätelaite. Kryptovaluutat ovat matemaattisiin malleihin, kryptografiaan perustuvia, internetissä toimivia valuuttoja, joista tunnetuin on Bitcoin. Muita kryptovaluuttoja eli altcoineja on kuitenkin satoja, ellei tuhansia, joista tunnetuimpia ovat Ethereum, Litecoin ja Ripple. Bitcoin on lähivuosina saanut runsaasti huomiota lehdistöissä, joka on tuonut sen suosioon muidenkin kuin tietotekniikasta kiinnostuneiden keskuuteen.

Opinnäytetyön tavoitteena on käydä tarkasti läpi lohkoketjun rakennetta enimmäkseen Bitcoinin näkökulmasta. Luvussa 2 käydään läpi Bitcoinia yleisesti. Luvussa 3 selvitetään lohkoketjun rakennetta ja sitä, että millaisia vaiheita transaktio käy läpi lohkoketjussa. Luvussa 4 käydään tarkemmin läpi, mitä lohkot sisältävät ja millä tavalla lohkon sisältöä hyödynnetään lohkoketjussa. Luvussa 5 kerrotaan esimerkkejä käyttökohteista, jossa lohkoketjuteknologiaa voidaan hyödyntää.

2 BITCOIN YLEISESTI

Bitcoin on luotiin koska tarvittiin virtuaalivaluutta, joka on aidosti vain kahden osapuolen välinen tapa siirtää varallisuutta osapuolelta toiselle. Bitcoinin loi nimimerkki Satoshi Nakamoto vuonna 2009, eikä hänen oikeaa henkilöllisyyttään tiedetä vieläkään. Bitcoinista kuultiin ensimmäisen kerran, kun Satoshi Nakamoto lähetti salaustekniikoista kiinnostuneiden sähköpostilistalle linkin nettisivulle, jossa oli pdf-tiedosto Bitcoin: ”Peer-to-Peer Electronic Cash System.”. Teksti kuvaa ongelmaa, jossa elektronisessa rahaliikenteessä täytyy edelleen luottaa kolmanteen osapuoleen. Yksi isoimmista ongelmista on se, että tietyissä olosuhteissa pystytään ujuttamaan maksuliikenteeseen kaksinkertaisia maksuja yhdestä lähteestä, kun maksu on varmennettu kertaalleen. Tekstissä kuvataan myös ongelmaksi se, että kun rahaliikenteessä tarvitaan kolmas osapuoli, niin siitä koituu käyttäjille lisää kuluja, jolloin esimerkiksi erittäin pieniä ”mikrotransaktioita” ei voida saada kannattavaksi. Lisäksi ongelmana on, että maksuja ei voida peruuttaa, joten tarvitaan yhä enemmän luottamusta rahan siirtoihin ja kaupankäyntiin. Ratkaisu on sellainen sähköinen maksujärjestelmä, joka käyttää kryptografista varmennus algoritmia, joka perustuu todistamiseen luottamuksen sijaan. Tällöin ketkä tahansa kaksi osapuolta voivat tehdä transaktioita keskenään ilman tarvetta kolmannelle osapuolelle. Siirrot, jotka ovat laskennallisesti epäkäytännöllisiä peruuttaa, ovat hyvä suoja kauppiaille ja ”escrow” palvelut ovat hyvä suoja kuluttajalle luottamuksen varmistamiseksi. (Peer-to-Peer Electronic Cash System, 2009.)

Nykyään Bitcoinilla tehdään keskimäärin 250 000 transaktiota päivässä. Netissä voi luoda oman lompakon alle minuutissa ja voit ostaa ja myydä useissa sadoissa pörsseissä virtuaalivaluuttaa tai vaihtaa niitä toisiin kryptovaluuttoihin. Kirjoitushetkellä kokonaisen Bitcoinin arvo on 2940 euroa. Maailmassa on 141 831 Bitcoineja maksuna hyväksyviä yrityksiä, joista Suomessa niitä on 65. Bitcoineja vaihtavia automaatteja on 4045, joista Suomessa 18. (Coinatmradar, 2018.)

Tekstissä käydään myös tarkemmin läpi teknisiä ominaisuuksia kuten siirtojen toteutumisen logiikka, Proof-of-Work -järjestelmää, blockchainia, muistinhallintaa ja yksityisyttä. Näistä käsitteistä tulee tarkempaa tietoa muissa osioissa.

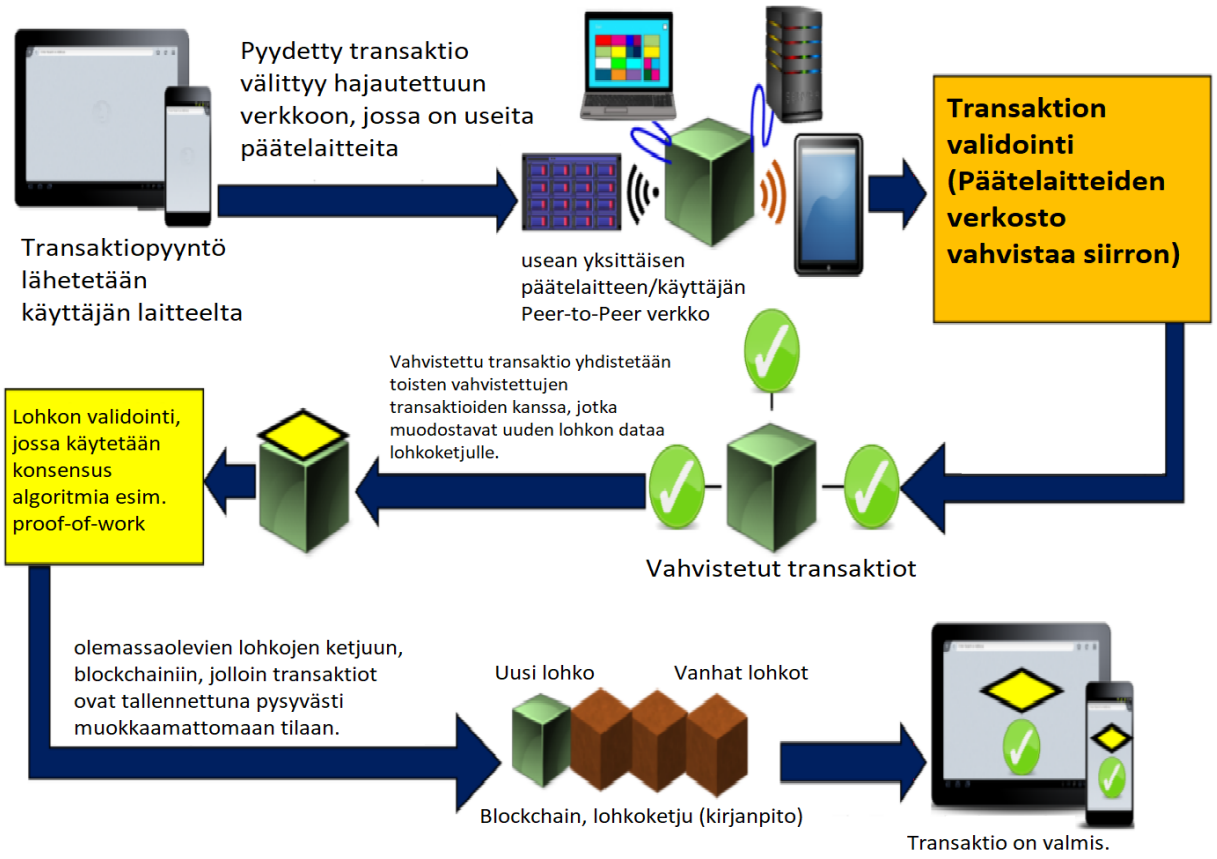
3 LOHKOKETJU

3.1 Lohkoketju yleisesti

Useimpien kryptovaluuttojen kuten Bitcoinin siirrot tapahtuvat jaetun, avoimen kirjanpidon kautta, jota kutsutaan lohkoketjuksi. Lohkoketju koostuu pienemmistä osista eli lohkoista, joihin tallennetaan pysyvästi kaikki viimeisimmät transaktiot. Kun lohko on täynnä transaktioita, se lisätään aikaisempien lohkojen perään muodostaen uuden lohkon lohkoketjussa. Lohkoa voisi verrata esimerkiksi vanhanaikaisen kirjanpidon sivuun, jonka täyttyessä se tulee jatkeeksi muiden kirjausten perään, ja siihen ei voi tehdä muutoksia, jos sinne jotain kirjataan. Lohkoketju tallentaa tiedot transaktioista, jotka ovat tapahtuneet verkon käyttäjien välillä ilman, että tarvitaan ollenkaan kolmatta osapuolta. Kirjanpidosta on kopio kaikilla, jotka ovat osallisia verkkoon. Lohkoketju käyttää julkisten avainten hallintajärjestelmää (Public Key Infrastructure = PKI) todentamiseen ja tunnistamiseen anonyymien osapuolten välillä. Kaikki transaktiot ovat digitaalisesti ”allekirjoitettu” lähettäjän salausavaimella. (What Is PKI, 2018)

Useat samanaikaiset transaktiot on ryhmitetty rakenteeseen, jota kutsutaan lohkoksi, jolla on uniikki tunniste.

Transaktioiden ja lohkon validointi voidaan tehdä täysin luottamatta käyttäjiin, kun käytössä on jaettu yhteinen kirjanpito, lohkoketju. Validointi tapahtuu enemmistön päätöksellä, jolloin yksittäinen epäluotettava taho ei pysty manipuloimaan lohkoketjuun tallennettavaa dataa. Bitcoinin tapauksessa lohkoketjuun uusien transaktioiden päivittämiseen käytetään proof-of-work algoritmiä, jossa louhijat käyttävät tietokoneen laskentatehoa löytääkseen tietyn, uniikin, muuttuvan tiiviste arvon, jota kutsutaan nonceksi, joka uusiutuu aina kun se on löydetty, keskimäärin 10 minuutin välein. Tästä muodostuu 10 minuutin lohkoaika. Tätä kutsutaan louhimiseksi. (BitcoinWiki 2018.) Louhinnan kautta, päätelaitteet kilpailevat siitä, että kuka löytää seuraavan lohkon tiivisteen arvon ja tähän investoidaan valtavasti rahaa laitteiden, laskentatehon ja sähkön muodossa, koska lohkon löytämisestä saa palkkioksi kryptovaluuttaa. Kuvassa 1 kuvataan ohkoketjuun tallentuvan siirron vaiheet.



(Kuva 1: Lohkoketjun yleiskuva – Mohanty, 2018)

3.2 Lohkoketjun komponentit

Tässä osiossa kerrotaan keskeisimmät komponentit lohkoketjusta ja niiden toiminnasta sekä käydään läpi lohkoketjun toiminnan eri vaiheita, jossa komponentit yhteistyössä tuottavat turvallisen tiedonvälityksen eri nodejen välillä ja luovat hajautetun lokin tehtyjen siirtojen välillä konsensus mekanismin avulla. Vaiheissa käytetään esimerkkinä tunnetuinta lohkoketjua Bitcoinia.

3.2.1 Epäsymmetrisen salauksen kryptografia (Asymmetric key Cryptograpy)

Lohkoketju käyttää julkisen ja yksityisen avainten salausalgoritmejä turvallisen toiminnallisuuden takaamiseen. Kaikkeen rahanvaihtoon tarvitaan digitaalinen lompakko (vähän niin kuin pankkitili), joka on suojattu käyttäjän yksityisellä avaimella, jolla voi tunnistautua ja päästä sisään omaan lompakkoonsa. Tämän lompakon julkinen avain on lom-

pakon osoite, jonka voi jakaa muille, kun haluaa vastaanottaa Bitcoineja. Julkisen avaimen voi vaihtaa vaikka jokaiselle siirrolle esimerkiksi yksityisyys syistä tai, jos haluaa yksilöidä ja tunnistaa anonyymiltä taholta tulleen siirron. (Hackernoon 2016.)

3.2.2 Transaktiot

Bitcoinissa jokainen transaktio tarkoittaa valuutan siirtoa nodelta toiselle. Kaikki nodet ovat tietoisia kaikkien muiden nodejen sen hetkisestä katteesta, koska jokaisella päätteellä on kopio koko lohkoketjusta, joka on loki, joka sisältää kaikkien transaktioiden historian.

Lohkoketju sallii tiedon jakamisen ja vaihtamisen nodejen välillä vertaisverkon (peer-to-peer) avulla. Tämä tiedonvaihto tarkoittaa niiden tietojen vaihtoa, jotka sisältävät siirtoon ja sen yksilöintiin liittyvää dataa nodejen välillä. Lähettävä node luo tämän datan ja "kuuluttaa" sen koko lohkoketjulle validoitavaksi. Lohkoketjun tila määräytyy näistä transaktioista, joita nodet jatkuvasti luovat ja joista lohkot koostuvat. Lohkoketjun tila vaihtuu jokaisen transaktion jälkeen ja kun transaktioita on useita sekunnissa, niin on tärkeää, että validoidaan ja tarkastetaan aidot siirrot ja hylätään väärennetyt.

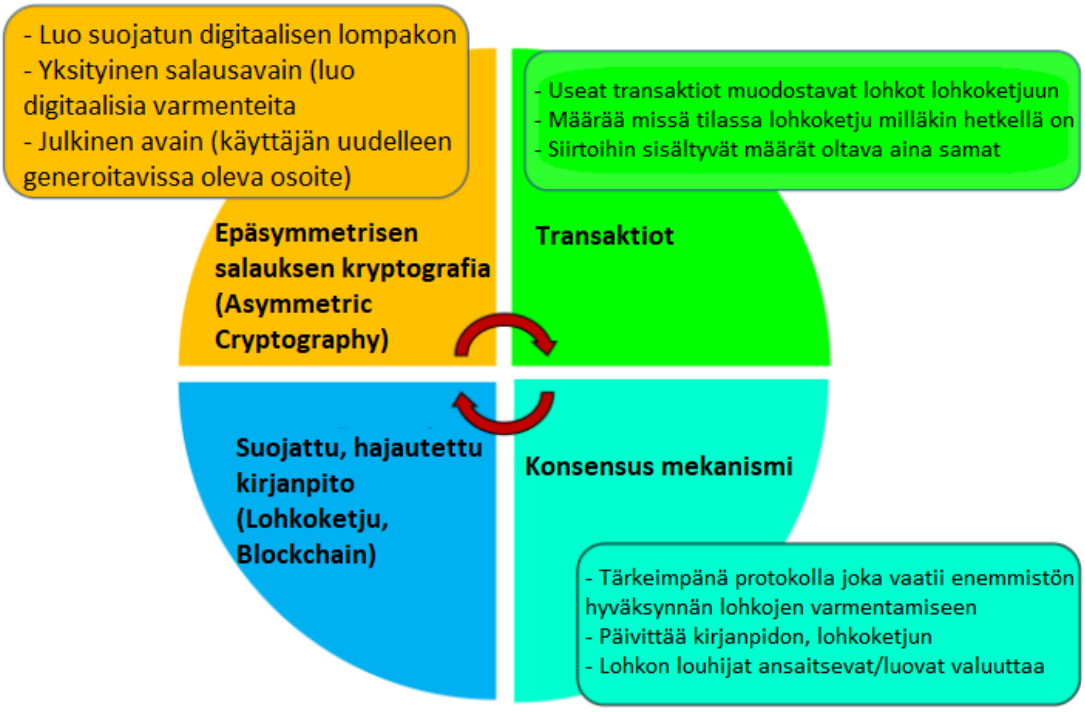
3.2.3 Konsensus mekanismi

Kun nodet aloittavat datan jakamisen ja vaihtamisen lohkoketjun kautta, niillä ei ole ketään keskitettyä tahoa, joka voisi ratkaista erimielisyyksiä, suojata tietoturvarikkomuksilta ja mekanismia seuraamaan varojen kulkua ja varmistamaan, että petokset, kuten kaksinkertaiset kulutushyökkäykset (double spending attacks) eivät ole mahdollisia. Kaikkien nodejen tulee hyväksyä kirjanpidon päivitystä varten luotua protokollaa, jossa siirtoja ei yksinkertaisesti voi hyväksyä osaksi lohkoketjua ilman enemmistöpäätöstä. Tätä kutsutaan konsensus mekanismiksi, jolla lohkot luodaan ja lisätään osaksi kirjanpitoa eli lohkoketjua.

Virtuaalisessa kaupankäynnissä voi päätyä tilanteeseen, jossa vastaanottaja on hyväksynyt ja verifioinut siirron jollakin virtuaalisella varmenteella. Kuitenkin voidaan päätyä tilanteeseen, jossa siirtoyhteyden varmentamisen jälkeen voidaan tehdä useampi perät-

käinen siirto samalla varmenteella, jolloin siirron lähettävä taho pystyy huijaamaan järjestelmää, että siirto on jo verifioitu ja näin ollen pystyy luomaan tyhjästä varmennettuja siirtoja. Tätä kutsutaan kaksinkertaiseksi kulutushyökkäykseksi.

Pääosin tätä varten Satoshi keksi ensimmäisenä maailmassa konsensukseen perustuvan hajautetun virtuaalivaluutan epäluotettavien nodejen välille. Tämä konsensus on nodejen välinen hyväksyntä, johon kuuluu lohkojen louhinta, jossa louhijat kilpailevat löytääkseen validin lohkon tiivisteen arvon, käyttäen tietokoneen laskentatehoa. Löytäjä saa palkkioksi bitcoineja, jotka luodaan uutena järjestelmään. Tästä lohkon tiivisteestä käytetään nimeä 'the proof of work' ja jos kaikki lohkoon sisältyvät siirrot ovat valideja, niin kaikki nodet hyväksyvät sen ja päivittävät kirjanpitoonsa eli lohkoketjuun kopion lohkosta. Lohkon muodostumisen voi jakaa kahteen suurempaan osaan, jotka ovat transaktion luonti ja varmentaminen sekä konsensuksen toteuttaminen ja lohkon validointi. Kuvassa 2 kuvataan lohkoketjun keskeisimmät komponentit.



(Kuva 2: Lohkoketjun keskeisimmät komponentit – Mohanty, 2018)

4. TRANSAKTION GENEROIMINEN JA VAHVISTAMINEN

Samaan verkkoon kytketyt käyttäjät tietävät toistensa osoitteen ennen siirron aloittamista. Kun uusi transaktio aloitetaan, se sisältää käyttäjän syöttämän Bitcoin määrän ja vastaanottajan Bitcoin osoitteen. Esimerkiksi Pekka haluaa siirtää 0,5 Bitcoinia Matille niin siirtoon sisältyy seuraavat tiedot:

- lähde, mistä lähettäjä on Bitcoininsa saanut
- siirrettävien Bitcoinien määrä
- Bitcoineja vastaanottavan julkisen avaimen tiiviste.

Transaktion lähde kertoo, mistä transaktioon siirrettävät kolikot ovat peräisin. Tarkemmin, se viittaa tiivisteen arvoon, josta saadaan tilasto siitä, että mistä Pekka on saanut 0,5 Bitcoinia, jonka hän haluaa siirtää Matille. Nämä voivat olla yksi tai useampi tapahtuma, jonka summa on 0,5 Bitcoinia. Sanotaan vaikka, että ne tulevat neljästä lähteestä, jotka ovat julkaistuja kirjanpidossa. Silloin seuraavalle siirrolle tulee neljä lähdettä syötteelle. Transaktio kohdistetaan Pekan haluamalla tavalla, tässä esimerkissä yhteen osoitteeseen, joka on Matin julkisen avaimen tiiviste, eli lompakon osoite. Transaktiot ovat uniikisti yksilöityjä transaktion ID:llä. Tämä on vielä ”allekirjoitettu” lähettäjän yksityisellä avaimella luodulla tunnisteella, jotta vastaanottajan päässä voidaan yksilöidä ja verifioida lähde, mistä siirto on tullut. Jos mitään näistä parametreistä muutetaan, se vaikuttaa transaktion ID:hen ja allekirjoitukseen ja jos jokin ei täsmää, niin transaktio hylätään.

4.1 Transaktion vahvistaminen

Kun Matin lompakolla havaitaan siirto, sen täytyy varmistaa, että ei ole kaksinkertaisia siirtoyrityksiä samoilla tunnisteilla ja että transaktio näkyy vahvistettavana siirtona lohkossa. Ennen kuin transaktio on vahvistettu, niitä ei pidetä luotettavina. Transaktio toteutuu vain silloin, jos Matti pystyy vastaanottamisen yhteydessä tarkistamaan seuraavat asiat:

a) Transaktioon viittaavan syötteen UTXO on kelvollinen eli ei ole kaksinkertaisia siirtoyrityksiä. UTXO (Unspent Transaction Output) on järjestelmä, joka määrittää Bitcoin osoitteen balanssin laskemalla käyttämättömän valuutan määrän saapuvien ja lähtevien transaktioiden perusteella. Kaksinkertaisia siirtoyrityksiä

Bitcoinissa estetään niin, että vasta sitten kun transaktio on tarkastettu sekä allekirjoituksen että lohkon kautta, niin varoja voidaan käyttää uudessa transaktiossa.

b) Vain se käyttäjä, jolla on lupa käyttää UTXO:ta, voi käyttää sitä myöhemmässä tapahtumassa. Vastaanottaja tarkistaa pätevän allekirjoituksen, joka vastaa UTXO-omistajan allekirjoitusta.
c) Viitattu transaktio on julkaistava kelvollisessa lohkossa. Se, että transaktio näkyy lohkossa tarkoittaa, että se on validi.
d) Arvon säilyminen on välttämätöntä, mikä tarkoittaa, että siirtojen aikana on pakollista, että syötteen UTXO:t on yhtä suuri kuin ulostulon UTXO:t. Tämä on yksi tärkeimmistä tekijöistä, jotka määrittelevät transaktion oikeellisuuden.

4.1.1 Omistusoikeuden vaatiminen

Jokainen transaktio tuottaa ulostulon, jonka valtuutetut vastaanottaja nodet voivat valtuuttaa julkisen avaimen tiivisteellä eli lompakon osoitteella. Tämä julkisen avaimen tiiviste on käyttäjän uniikki tunniste verkossa, joka samalla säilyttää käyttäjän yksityisyyden. Käyttäjät tarvitsevat yksityisen avaimensa hallitakseen omia Bitcoinejaan. Vain ne käyttäjät, jotka voivat luoda kelvollisia allekirjoituksia yksityisillä avaimillaan, voivat luoda kelvollisia siirtoja. Näin ollen julkinen ja yksityinen avain ovat oleellinen osa sille, että käyttäjä voi lunastaa varansa.

4.1.2 Konsensus, louhinta ja lohkon validointi

Kun vastuussa olevaa, luotettavaa, kolmatta osapuolta ei ole, niin nodet eli päätelaitteet noudattavat samaa konsensusta siitä, että kuinka lohkot ja transaktiot hyväksytään tai hylätään, jotta myöhemmässä vaiheessa ei aiheudu ristiriitoja. Tämä yhteisymmärrys saavutetaan "proof-of-work"in avulla, joka osoittaa, kuinka paljon töitä on tehty lohkon validoimiseksi. Kryptografinen/matemaattinen ongelma on ratkaistava minkä tahansa lohkon hyväksymiseksi, eli lohkon lisäämiseksi lohkoketjuun. Tämä toimii niin, että nodet kokoavat hyväksytyt transaktiot lohkoon, ja käyttävät omia resurssejaan (laskentatehoa, sähköä) etsiäkseen jokaiselle lohkolle uniikkia tiiviste arvoa. Tätä tapahtumaa voitaisiin verrata vaikka lottoamiseen, jossa laitteet eli nodet kilpailevat siitä, että kuka arvaa no-

peiten oikean lottorivin. Lohko sisältää mielivaltaisen nonce arvon, edellisen lohkon tiivisteen, Merkle-juuren tiiviste arvon lohkoon listatuista transaktioista, aikaleiman ja lohkon version. Lohkon sisältöä käydään läpi tarkemmin myöhemmin. Lohkon validointiin tarvitaan tiivistetysti seuraavat vaiheet:

1. Kaikki transaktiot lohkossa verifioidaan. Yksilöllisen tarkastuksen jälkeen transaktioiden aikajärjestys ja yksittäisten transaktioiden väliset viittaukset vahvistetaan.
2. Edellisen lohkon tiiviste, johon viitataan nykyisessä lohkossa, on yhä voimassa. Tämä voidaan tarkistaa genesis lohkosta.
3. Aikaleiman oikeellisuus tarkastetaan.
4. Nykyisen lohkon "proof-of-work" arvo on validi.

4.2 Lohkon ylätunniste

Kaikki lohkot sisältävät ylätunnisteen eli headerin ja sisällön eli transaktion. Headerissa on tärkeitä tiivistearvoja lohkosta, joiden avulla voidaan nopeasti laskea siirtojen oikeellisuus, ilman että tarvitsee tietää kaikkea lohkon sisältöä. Kuvassa 3 esitetään headeriin sisältyvät tiedot.

Size	Field	Description
4 bytes	Version	The Bitcoin Version Number
32 bytes	Previous Block Hash	The previous block header hash
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty target for the block.
4 bytes	Nonce	The counter used by miners to generate a correct hash.

(Kuva 3: Lohkon headerin rakenne – Cryptocompare, 2017)

Version: kuvaa versionumeroa, joka muuttuu aina kun lohkoketjun protokollaan tehdään muutoksia.

Previous Block Hash: kuvaa edellisen lohkon tiivisteen arvoa. Tällä lohkot ovat yhdistettynä toisiinsa.

Merkle Root: tiiviste, joka varmistaa transaktioiden aitouden. Tiivisteen arvo lasketaan kaikista transaktioista, jotka tulevat kyseiseen lohkoon. Tästä on hyötyä, kun louhinnalla varmistetaan transaktioita; ei tarvitse käydä läpi koko lohkon sisältöä, kun headerista saadaan varmistettua siirtoon menevien Bitcoinien aitous ja alkuperä. (cryptocompare.com 2018)

Timestamp: UNIX aikaleima, jolloin lohko on luotu (kuluneiden sekuntien määrä päivämäärästä 01.01.1970 00:00:00 UTC).

Difficulty Target: arvo, joka määrää kuinka epätodennäköistä on löytää (louhia) seuraava lohko. Arvo muuttuu sen mukaan, kuinka nopeasti edellinen lohko louhittiin. Tämän avulla lohkoketjun algoritmit pitävät huolen, että vaikka louhintateho kasvaa, niin keskimääräinen aika lohkon louhimiseen on 10 minuuttia. (cryptocompare.com 2018.)

Nonce: muuttuva arvo, joka auttaa siinä, että seuraavan lohkon tiiviste ei ole arvattavissa, eikä noudata tiettyä kaavaa (cryptocompare.com 2018).

4.3 Verkon toimintavaiheet

Blockchain verkon toimintavaiheet kuvataan niiden suoritusjärjestyksen mukaisella tavalla seuraavanlaisesti:
Tapahtumalähetys: Osapuolten välillä ei saa olla suoria transaktioita, vaan nämä transaktiot on julkaistava koko verkolle tarkastettavaksi.

Transaktioiden keruu ja validointi: Nodet vahvistavat kaikki transaktiot kohdan 4.1.1 vaiheiden mukaisesti ja kertyvät lohkoon lohkokoon määrittelemällä tavalla (Bitcoinissa 1MB).

Jatkuva konsensusprotokolla: Lisätäkseen lohkon lohkoketjuun nodet käyttävät resurssejaan löytääkseen hankalaksi löydettävän, tietoturvallisuutta lisäävän proof-of-workin tiivisteen arvon. Kun tämä on ratkaistu, niin lohko voidaan lähettää verkkoon.

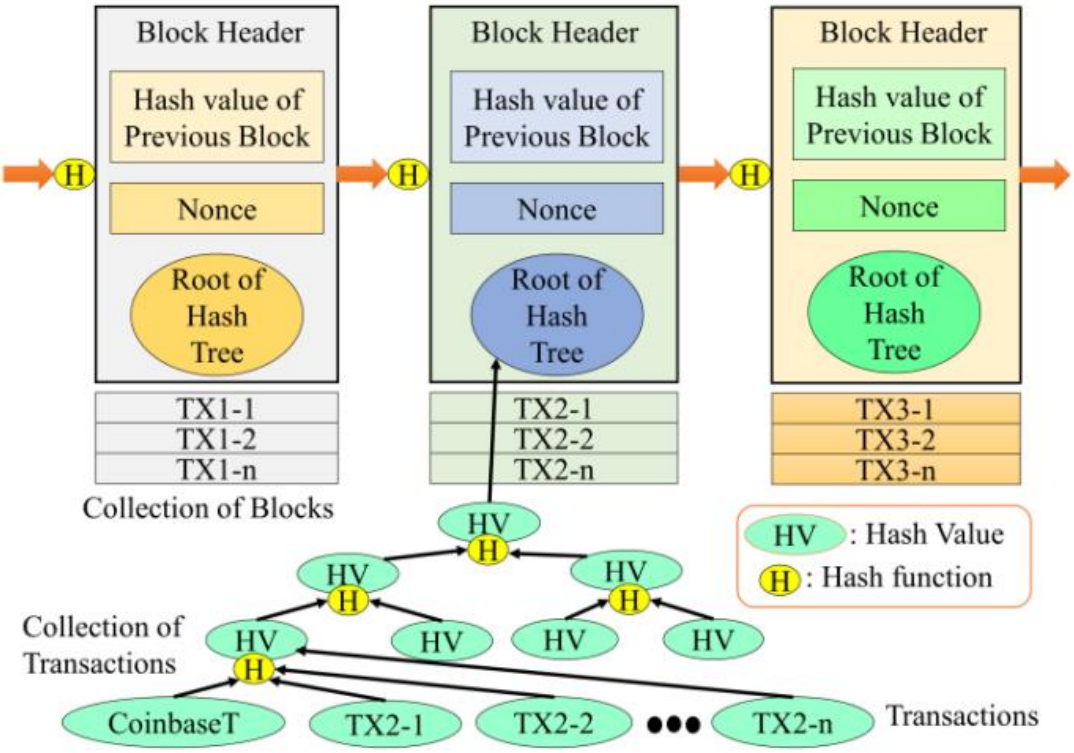
Lohkon hyväksyminen ja ketjun päivitys: Kun nodet vastaanottavat lohkot omaan kirjanpitoonsa, kaksi skenaariota voi tapahtua:

1. Joko nodet hyväksyvät lohkon, edellyttäen, että kaikki sen sisältämät transaktiot ovat valideja ja laskettu proof-of-work on oikein. Nodet osoittavat hyväksyntänsä lisäämällä kopion lohkosta omaan kopioituun kirjanpitoonsa ja jatkaa seuraavan lohkon etsimistä. Tässä vaiheessa aiemmin etsitystä lohkosta tuleekin edeltävä lohko ja sen tiivisteestä tulee edellisen lohkon tiiviste. Jos useampi louhija löytää validin ratkaisun lohkoon samanaikaisesti, niin vain pidemmän lohkoketjun omaavan ratkaisu katsotaan päteväksi. Näin lohkoketjusta tulee väärentämätön, ja kerran tehdyt muutokset eivät voi olla muutettavissa. (coindesk.com 2017).

2. Jos lohkossa on hylättyjä transaktioita tai hylätty proof-of-work -tiiviste, niin koko lohko hylätään ja jatketaan validin lohkon etsimistä.

Palkkioiden ansainta: Louhijat ansaitsevat palkkion, kun lohko hyväksytään, tämä tekee louhijoista rehellisiä, koska ainoa tapa saada henkilökohtaista hyötyä järjestelmän pyörittämisestä, eli louhimisesta, on yrittää saada itselleen lohkon luonnin yhteydessä tullut ennalta määrätty palkkio.

Kuvassa 4 esitetään lohkoketjun verkon toimintavaiheet.



(KUVA 4: Verkon toimintavaiheet – Smohanty 2018)

5. LOHKOKETJUN KÄYTTÖKOHTEET

Blockchainillä on mahdollisuus mullistaa monenlaisen käyttökohteen ja verkon turvallisuuden, vakauden ja läpinäkyvyyden edellyttäen, että sitä käytetään oikein ja oikeanlaisiin käyttökohteisiin.

5.1 Lohkoketju rahansiirrossa

Rahansiirto on erittäin tärkeä ja arkinen prosessi, joka voi esimerkiksi eri pankkien tai maiden välillä muuttua kalliiksi ja hitaaksi prosessiksi, koska väliin tulee turhan monta välittäjää/pankkia hidastamaan ja ottamaan rahallista osuutta maiden välisistä transaktioista. Rahan siirrossa pankista toiseen se voi parhaimmillaan mennä useankin valuutanvaihdon ja pankin läpi, ennen kuin saat rahat käyttöösi. Voidaan käyttää esimerkiksi Western Union -palveluja, jotka ovat nopeita, mutta myös kalliita ja yksinkertaistaa tätä prosessia katkaisemalla tarpeettomat välittäjät, jolloin kuluttajalle jää enemmän käteen valuutan vaihtokustannusten vähentyessä ja välikäsien osuuksien laskemisen ansiosta. Pahimmillaan nämä kustannukset voivat nousta jopa 20 prosenttiin, lohkoketjun avulla nämä kustannukset alenevat 2-3 prosenttiin kokonaismäärästä.

5.2 Lohkoketju ja IoT

Lohkoketjua voidaan käyttää apuna ylläpitämään jatkuvasti kasvavaa määrää sensitiivistä, suojattua dataa tietokannassa. Lohkoketjussa oleva data on suojassa muutoksilta, jotka tahallisesti tai tahattomasti saattaisi tulla muunnetuksi. Esimerkiksi nykyaikaisessa varastohallissa voisi olla säilössä tavaraa, jotka vaativat tarkkaa lämpötila tai sijaintitietoa. Automatisoidulle varastonhallinnalle on tärkeää, että siinä toimivat komponentit ymmärtävät, milloin varastoitu tuote on kelvoton vaikkapa viallisen jäähdytyksen takia. Jos kyseessä on vaikka hyllyyn ja hyllystä tavaraa kuljettava robotti, niin on tärkeää olla helposti käytettävissä oleva yhteinen kirjanpito varaston tilatiedoista. Kirjanpito ei korruptoidu yksittäisistä virheistä, koska se on muokkaamaton, eikä se voi kaatua, vaikka yksittäinen node kaatuisi, koska kaikilla on kopio samasta lohkoketjusta järjestelmässään. Li-

säksi kuluttajalle olisi mahdollista todistaa lohkoketjusta, että tuote on ollut asianmukaisesti jäähdytettynä koko elinkaarensa ajan, koska siitä on koskemattomassa tilassa olevaa dataa tallennettuna lohkoketjuun.

5.3 Lohkoketju kiinteistöissä

Transaktiot kiinteistö kaupoissa voi olla hankalaa, läpinäkymätöntä ja kallista erilaisten välittäjien, yritysten, valtion toimien, tarkastajien ja arvioijien vaatimien toimien takia. Lohkoketju mahdollistaa jokaiselle kiinteistölle ja sen osalle oman vastaavan digitaalisen osoitteen, joka sisältää läpinäkyvää tietoa esimerkiksi kiinteistön käyttöasteesta, rakennuksen suorituskyvyistä, fyysisistä ominaisuuksista, remonttitiedoista ym. rakennuksen tiedoista. Lohkoketjun avulla kaikki tietoja tarvitsevat tahot saavat yhteisestä kirjanpidosta haluamansa tiedot, ja tiedot säilyvät muokkaamattomana järjestelmässä ikuisesti.

6. POHDINTA

Lohkoketju on avoimen lähdekoodin perustuva mullistava teknologia, joka tarkoilla ja älykkäillä algoritmeillä pystyy ratkomaan sen, mitä pankit tekevät siirrettäessä varallisuutta paikasta toiseen. Tätä mullistavaa innovaatiota voi olla hankala ymmärtää, jos ei ole kiinnostusta käyttää suurta määrää aikaa asian tutkimiseen. Siksi on tärkeää, että lohkoketjuun perustuvia sovelluksia ja käyttökohteita tulee jatkuvasti lisää, koska silloin hyödyt konkretisoituvat niillekin, jotka eivät ole kiinnostuneita siitä, että mitä kryptovaluuttojen ”konepellin” alla tapahtuu. Teknologian mennessä eteenpäin laitteet tulevat yhä enemmän keskustelemaan keskenään. Tänä päivänä ja varsinkin tulevaisuudessa merkittävä osa laitteista, kulutustavarasta ja koko ympäröivä maailma kerää dataa hyödyntääkseen sitä johonkin. Siksi yhä suurempi osa maailmasta tulee hyötymään lohkoketjun tarjoamasta automaattisesta datan keruu- ja säilömislogiikasta.

Lohkoketjusta ja Bitcoinista tulee yleensä ensimmäisenä mieleen valuutta ja sijoittaminen, mutta todellisuudessa sillä on paljon muitakin käyttökohteita. Se, että Bitcoin jaettiin julkistamishetkellä täysin avoimena lähdekoodina, on mahdollistanut sen, että sitä on voitu jatkokehittää muihinkin käyttötarkoituksiin. On kiehtovaa nähdä, että mihin kaikkeen lohkoketjuun jatkossa tullaan hyödyntämään. Omasta mielestäni lohkoketjua voisi verrata internetin alkuaikoihin, jolloin vain häviävän pieni osa ihmisistä käytti sitä, koska sille ei enemmistön näkökulmasta löytynyt tarpeeksi käyttökohteita. Lohkoketju etsii vielä paikkaansa maailmassa, koska suurin osa käyttäjistä käyttää sitä vain sijoitustarkoitukseen.

Lohkoketju on kuitenkin nerokas ja moneen tietotekniseen tiedonsiirtoon ja varmentamiseen liittyvä merkittävä innovaatio, ja voisi sanoa, että oikeissa olosuhteissa täysin murtamaton, vaikka se toimiikin täysin itsenäisesti. Tästä todisteena toimii se, että sitä ei ole kukaan, edes parhaimmat hakkerit, pystyneet vieläkään murtamaan, vaikka onkin täysin avointa lähdekoodia.

LÄHTEET

Satoshi Nakamoto, Bitcoin open source implementation Luettu 09.09.2018 http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Luettu 09.09.2018 https://bitcoin.org/bitcoin.pdf

Blockchain Info Luettu 29.10.2018 https://blockchain.info

Bitcoinwiki, Luettu 26.07.2018 https://en.bitcoin.it/wiki/Proof_of_work

The Truth About Bitcoin. Luettu 18.10.2018. https://hbr.org/2017/01/the-truth-about-blockchain

D. Puthal, N. Malik, S.P. Mohanty, E.Kougianos, G.Das. Everything you Wanted to Know about the Blockchain. Luettu 09.11.2018 http://www.smohanty.org/Publications_Journals/2018/Mohanty_IEEE-CEM_2018-Jul_Blockchain.pdf

X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems" Luettu 26.07.2018

What Is a Block Header in Bitcoin, Luettu 29.10.2018 https://www.cryptocompare.com/coins/guides/what-is-a-block-header-in-bitcoin/

Symmetric and asymmetric key cryptography, Luettu 09.12.2018 https://hackernoon.com/symmetric-and-asymmetric-encryption-5122f9ec65b1

How does blockchain technology work, Luettu 01.12.2018 https://www.coindesk.com/information/how-does-blockchain-technology-work