Haaga-Helia
ammattikorkeakoulu Oy

Kryptovaluuttojen kvanttiuhat

Kalle Tyllilä

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2021

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä(t)
Kalle Tyllilä

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Kryptovaluuttojen kvanttiuhat

Sivumäärä
36

Ensimmäinen yleisesti tunnettu lohkoketjuteknologiaan perustuva käytännön sovellus oli kryptovaluutta bitcoin. Lohkoketjussa tieto hajautetaan ja tietoa ylläpitävät niin kutsutut louhijat ja lohkoketjuverkon muodostaa samassa verkossa operoivat tehokkaat tietokoneet.

Eräs lohkoketjuteknologian tärkeimmistä ominaisuuksista on, että ketjun lohkoihin voidaan lisätä vain uutta tietoa, eikä tietoa pysty enää jälkikäteen muuttamaan ja se on suljettu muutoksilta, jonka muuttumattomuuden varmistaa ns. tarkiste.

Lohkoketjun sisältämiin lohkoihin voidaan tallentaa teoriassa mitä tahansa tietoa, joten lohkoketjuteknologialla voidaan toteuttaa esimerkiksi valtakunnallinen äänestys luotettavasti. Lohkoketjuteknologialla kyetään eliminoimaan väärinkäytösten ja väärennösten mahdollisuus.

Kvanttitietokoneet kuitenkin muodostavat tulevan uhan monimutkaisemmillekin salausmenetelmille ja perinteiset salausmenetelmät, kuten RSA ja Elliptisen käyrän salausmenetelmä ovat uhattuna. Kvanttitietokoneiden laskentateho ja kvanttilaskenta kvanttialgoritmeillä kuten Shorin- tai Groverin algoritmeilla voidaan nähdä sekä turvallisuutta lisäävänä, että turvallisuutta uhkaavana mahdollisuutena.

Kryptovaluutta kiinnostaa kyberrikollisia ja yleisimmät niiden suojauksiin kohdistuvat uhat ovat 51%-hyökkäys, DDOS-hyökkäys sekä BGP-hyökkäys. Kryptovaluuttojen kvanttiuhat voidaan puolestaan jakaa kahteen erilaiseen algoritmiluokkaan, joista toinen rakentuu Shorin algoritmin ja toinen Groverin algoritmin hyödyntämiseen.

Riskievaluaatiossa verrataan tunnetuimpien kryptovaluuttojen suojautumispotentiaalia Shorin sekä Groverin algoritmeja hyödyntäviä kvanttihyökkäyksiä vastaan ja läpikäydään kryptovaluuttojen riskiluokitukset.

Kvanttivarmoiksi kryptovaluutoiksi nostetaan Mochimo ja QRL. Mochimo suojautuu Chain Crunch ™ teknologian taakse ja QRL suojautuu hajautus-salaukseen perustuviin digitaalisiin allekirjoituksiin.

Pohdintaosiossa todetaan, että kvanttivarmat kryptovaluutat ovat arvokas tulevaisuuden sijoituskohde ja se karkea tosiasia, että kvanttitietokoneiden käytännön implementaatiot tulevat luomaan uusia ja ennalta tuntemattomia uhkia ja haavoittuvuuksia.

Asiasanat
Lohkoketju, kryptovaluutta, kvantti, algoritmi, kvanttitietokoneet, salausmenetelmä

Sisällysluettelo:

Johdanto.

Tämän opinnäytetyön tarkoituksena on käsitellä kryptovaluuttojen kvanttiuhkia mahdollisimman monipuolisesti ja monelta näkökannalta. Luoda helposti lähestyttävä kokonaisuus kryptovaluuttojen turvallisuuteen ja etenkin siihen, kuinka kvanttitietokoneet tulevat uhkaamaan kryptovaluuttoja ja niiden tulevaisuutta.

Kryptovaluutat ja lohkoketjut ovat sanoina tulleet tutuiksi uutisista ja alan lehdistöstä. Kuitenkin monelle on epäselvää, kuinka lohkoketjut toimivat ja mihin perustuu kryptovaluuttojen arvo. Kryptovaluuttojen arvon voidaan katsoa perustuvan pitkälti niiden salausteknologioiden turvallisuuteen, jotka suojaavat kryptovaluuttaa. Lisäksi krypto-valuutan arvoa nostaa sen potentiaali mahdollisena arvonsäilyttäjänä muuttuvassa maailmassa. Tämä turvallisuus, joka perustuu kryptografiaan on kuitenkin uhattuna uusien teknologisten innovaatioiden johdosta, joista tehokkaat kvanttitietokoneet ovat suurin tunnistettu uhka.

Kvanttitietokoneiden- ja kvanttimatematiikan-teoriat ovat jo varsin vanhoja käsitteitä, mutta ne ovat juuri nyt ajankohtaisempia, kuin koskaan aikaisemmin. Tämä opinnäytetyö käsittelee sitä, minkälaisia teoreettisia turvallisuusuhkia on olemassa, miten niiltä suojaudutaan ja minkälaisia ovat ns. kvanttivarmat kryptovaluutat ja millä tekniikoin ne ovat suojatut.

Tämä tutkimustyö ei käsittele yksityiskohtaisesti matemaattisia konsepteja kryptovaluuttojen turvallisuuden taustalta, vaan yrittää luoda lukijalle yhdenmukaisen ja kompaktin tietopaketin kryptovaluutoista sekä niiden turvallisuudesta.

Tätä työtä viimeisteltäessä on uutisissa kerrottu Suomeen rakennettusta ensimmäisestä kvanttitietokoneesta. Uutisen mukaan kvanttitietokone on VTT:n ja suomalaisen IQM:n (start-up) yhteistyön tulos. Eikä maailmalla tiedetä olevan kuin yhteensä noin kymmenen vastaavaa konetta, mikä antaa hyvän perspektiivin kvanttitietokoneiden yleisyydestä . Tilanne tulee kuitenkin muuttumaan pian ja koneita tulee lisää. Tältä kannalta katsottuna ajoitus tämän opinnäytetyön kirjoittamiselle on hyvä.

1.0 LOHKOKETJUTEKNOLOGIAN PERUSTEET

Lohkoketjuteknologian kehitti Satoshi Nakamoto nimellä esiintynyt henkilö tai ryhmä henkilöitä. Ensimmäinen tunnettu lohkoketjuteknologian käytännön sovellutus *I.* bitcoin tuli laajempaan tietoisuuteen vuonna 2008.

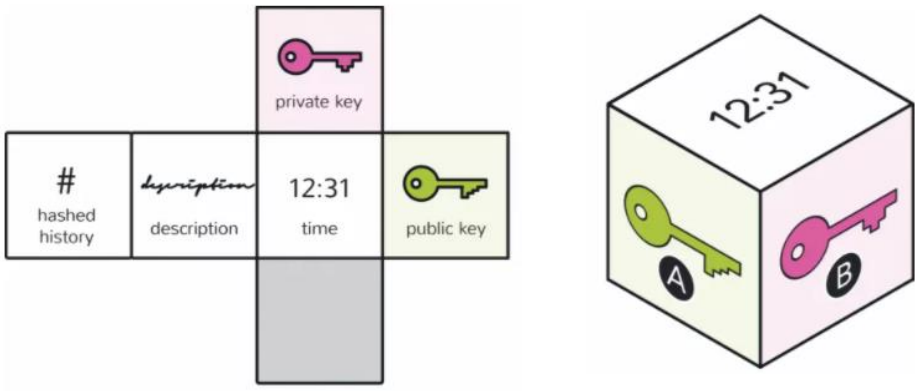
Lohkoketjuteknologialla tuotetaan hajautettu tietokanta, joka koostuu palvelimista eli solmuista (node). Bitcoin-louhijat liittävät ketjuksi lohkoja jotka sisältävät ainakin tiivisteen, aikaleiman sekä hyväksytyn transaktion tiedot.
*(*Heino E, Kaskinen N., Kinnunen S. ym**,** 24-25*)*

Lohkoketjun voi ajatella tilikirjana, jolla ei ole yhtä haltijaa, vaan kaikilla solmuilla on kopio tilikirjasta ja sen sisältämistä transaktiotiedoista. Tilikirjan hajauttaminen tuo turvallisuutta sekä luottamusta lohkoketjun kaikille osapuolille. Kun tilikirja on hajautettu niin siihen kirjattuja tietoja ei voida manipuloida eikä tilikirjaa pystytä tuhoamaan verkon ulkopuolisella kyberhyökkäyksellä.

Lohkoketjuja ylläpitävät niin kutsutut louhijat, lohkoketju verkon muodostaa samassa verkossa operoivat tehokkaat tietokoneet. Tietokoneet luovuttavat laskentatehoaan ja samalla kilpailevat siitä, kuka verkossa saa ensimmäisenä ratkaistua matemaattisen yhtälön uuden lohkon luomiseksi. Verkkoa ylläpitävät louhijat saavat uuden lohkon luomisesta korvaukseksi kryptovaluuttaa. Louhijat siis luovat uusia lohkoja ketjuun joita solmut säilövät tilikirjassaan. *(Northcrypto)*

1.1 Lohkon tarkiste/tiiviste

Bitcoinin toimintaperiaatteessa lohkon sisältämä tarkiste, jota solmuverkossa olevat louhijat yrittävät ratkaista on SHA-256-algoritmia, joka tuottaa aina 256-bittisen tarkisteen. Uuden ketjuun liitettävän lohkontarkisteen tulee sisältää myös edellisen lohkon lohkontarkisteen, sekä nonce muuttujan verran nollia. Koska suuri määrä nollia on 256-bittisen tarkisteen algoritmissä harvinaisia joutuu louhijat käymään miljoonia mahdollisia nonce-arvoja läpi ennen sopivan nonce-arvon löytymistä.
(*Karhunen 2018, 9)*



(kuva1, visualisointi lohkosta)

SHA-256 kryptografsella hajautusfunktiolla pystytään käytännössä luomaan mistä tahansa sanasta tai numerosta tarkiste. Lohkoketjuteknologia perustuu tämän SHA-256 hajautusfunktion ympärille. Alla olevassa merkkijonossa on esimerkki siitä, miltä sana *"tarkiste*" näyttää kun se on ajettu SHA-256 algoritmin lävitse:

"*tarkiste"* =
4c6658c4523d84c38f33d08ec6aed0d2cf0c90f6866393554f15caaddd51c2c7

Eräs lohkoketjuteknologian tärkeimmistä ominaisuuksista on se, että ketjun lohkoihin voidaan lisätä vain uutta tietoa. Lohkossa olemassa olevaa tietoa ei voi enää jälkikäteen muuttaa ja se on pysyvästi suljettu muutoksilta. Lohkojen muuttumattomuuden varmistaa tarkiste. Tarkiste sisältää yhteenvedon edellisen lohkon sisältämästä datasta, joten aiempien lohkojen muokkaaminen jälkikäteen on käytännössä mahdotonta. *(Virtuaalivaluutta)*

1.2 Konsensus

Konsensuksessa kolmannen osapuolen sijasta, verkon solmut sopivat transaktion hyväsymisestä. Uuden lohkon syntyminen vaatii viimeisenä vaiheena kaikkien lohkoketjuverkon solmujen yksimielisyyden lohkon sisällöstä. Kun muut solmut ovat hyväksyneet uuden transaktion, tarkisteen sekä aikaleiman syntyy uusi lohko, joka lisätään lohkoketjun viimeiseksi lohkoksi.

Lohkoketjun sisällöstä vallitsee nyt yksimielisyys ja louhijat voivat siirtyä uuden tarkisteen laskentaan. *(*Heino E, Kaskinen N., Kinnunen S. ym, 26 *)*

1.3. Älysopimukset

Lohkoketjuteknologia mahdollistaa ehdollistettujen sopimusten luomisen, joita kutsutaan älysopimuksiksi (smart contract). Lohkoketjuun voidaan ohjelmoida jokin ehto, jonka toteutuessa tapahtuu transaktio tai digitaalinen tapahtuma. Nämä ehdot sekä transaktiot voivat käytännössä olla mikä tahansa digitaalinen tapahtuma, joka ohjelmoidaan automaattisesti suoritettavaksi. Älysopimuksen käytännön sovellutus voi olla korvata välikäsi eli kolmas osapuoli kahden tuntemattoman toimijan välille. Tämä antaa sopimuksen molemmille osapuolille luotettavan mahdollisuuden kaupankäyntiin. Älysopimuksen tärkein ominaisuus on se, että ohjelmoitua ehtoa ei voida jälkikäteen enää manipuloida. (Bitcoinkeskus, 2020)

1.4 Julkinen ja yksityinen avain

Hajautetun tilikirjan järjestelmässä omistajuuden todennettavuus on vaikeampaa, koska omistajuutta ei valvo yksittäinen taho kuten pankki. Yksityisellä avaimella voidaan todentaa muille lohkoketjuverkon jäsenille, että transaktion tehnyt käyttäjä todella omistaa transaktiossa käytetyt varannot. Julkista avainta käytetään transaktioiden vastaanottamiseen jonkun toisen käyttäjän yksityisenavaimen kanssa synergiassa. Tätä kutsutaan digitaalisensignatuurin järjestelmäksi.

1.5 Pohdintaa lohkoketjun sovellutuksista

Lohkoketjun sisältämiin lohkoihin voidaan tallentaa teoriassa mitä tahansa tietoa. Näin ollen lohkoketjuteknologialla on lukemattomia määriä erilaisia sovellusmahdollisuuksia. Lohkoketjuteknologian tärkeimpiä tulevaisuuden sovellutuksia voisivat olla erilaiset yhteiskunnallista luottamusta ja läpinäkyvyyttä lisäävät projektit. Lohkoketjuteknologian sovellutuksella voidaan esimerkiksi toteuttaa valtakunnallinen äänestys luotettavasti. Koska lohkoketjun historiaa ei voi yksikään taho jälkikäteen muuttaa, on se oivallinen teknologia erilaisten omistajuuksien autentikoimiseen sekä korruptioiden, väärinkäytösten ja väärennösten vähentämiseen.

1.6 Avaimien säilyttäminen

Yksi potentiaalisten haavoittuvuuksien ilmentymä on kryptovaluuttalompakot. Kryptovaluuttalompakossa ei vastoin yleistä käsitystä säilytetä itse kryptovaluuttaa vaan transaktioissa käytettyjä avaimia. Lompakkoja on erilaisia ja niillä on erilaisia haavoittuvuuksia. Avaimia voidaan säilyttää ohjelmistossa, laitteistossa, pilvipalveluissa mutta kaikkein turvallisin tapa on avaimien kirjoittaminen paperille ja paperin huolellinen säilyttäminen. Hyvänä turvallisuuskäytäntönä pidetään myös avainten säilyttämistä laitteessa, jota ei ole yhdistetty internettiin.
(Bult 2019 , 19)

2.0 SALAUSMENETELMÄT

2.1 RSA

RSA salaus kehitettiin 1970-luvulla digitaalisten transaktioiden suojaamiseksi ja se oli ensimmäinen *asymmetrinen salausmenetelmä*. RSA menetelmän perustuu Whitfield Diffien ja Martin Hellmanin ideaan julkisen avaimen kryptografiasta. RSA salauksen käytännön sovellutuksen kehitti kuitenkin Ron Rivest, Adi Shamiri ja Leonard Adleman. (Joutsjoki 2019, 5)

RSA:ssa käytetyt matemaattiset algoritmit ovat suunniteltu niin, että salaus on helppoa luoda, mutta erittäin vaikeaa tai lähes mahdotonta purkaa klassisella tietokoneella. Digitaalisten transaktioiden vastaanottaminen sekä lähettäminen vaatii sen, että transaktiolla on kaksi osoitetta. Näitä osoitteita kutsutaan nimillä julkinen avain (public key) sekä yksityinenavain (private key). Julkista avainta käytetään transaktioiden vastaanottamiseen ja se on nimensä mukaisesti julkinen, koska siinä ei ole mitään salaamisen arvoista. Yksityistä avainta käytetään transaktioiden lähettämiseen ja se on nimensä mukaisesti salainen.

Koska julkinen avain on luotu yksityiseen avaimeen perustuen, on niillä matemaattinen korrelaatio toisiinsa. Kryptovaluuttojen säilyttäminen bittilompakoissa sekä transaktiot niiden välillä tapahtuu RSA-salaukseen perustuvilla avaimilla.

Kun osapuoli A haluaa lähettää osapuolelle B transaktion, luo osapuoli A yksityiseen avaimeensa perustuvan julkisen avaimen

$$a_{pub} = \boldsymbol{f}(a_{priv})$$

Ja lähettää sen osapuolelle B. Osapuolen B vastaanotettua A:n julkisen avaimen a_{pub} yhdistää hän sen oman b_{priv} avaimen kanssa luodakseen salaisen arvon c.

$$c = \boldsymbol{f}(a_{pub}, b_{priv}).$$

Osapuoli B suorittaa saman toimenpiteen, jolloin A:lla on sama arvo salaiselle c:lle.

$$c = \boldsymbol{f}(b_{pub}, a_{priv})$$

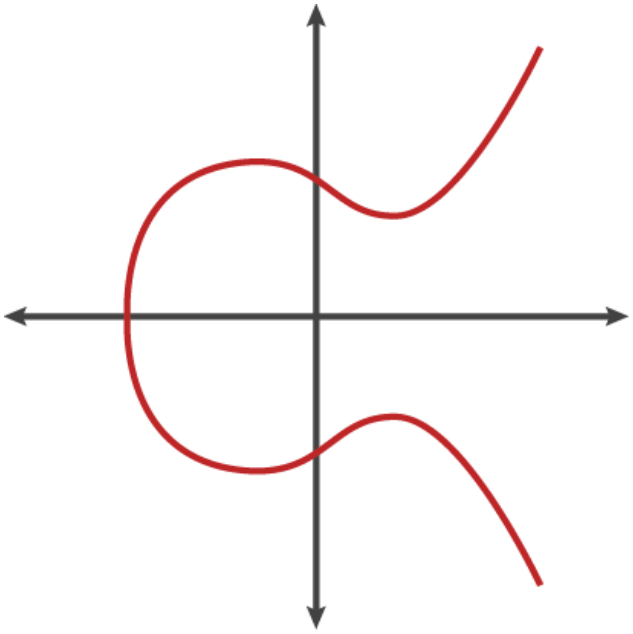
Nyt osapuolet A ja B ovat luoneet yhteisen salaisuuden, salausavaimen c, jota voidaan käytttää esimerkiksi AES-salaustekniikan salausavaimena.
(Joutsjoki 2019, 6).

2.2 Elliptisen käyrän salausmenetelmä (ECDSA & ECC)

Elliptinen käyrä on matemaattinen objekti, jolla kuvataan käyrää kaksiulotteisessa avaruudessa. Elliptisten käyrien käyttäminen julkisen avaimen salausmenetelmänä on edullista pienen avain koon sekä nopean toiminnallisuuden takia.

4096 bitin RSA-salaus vastaa turvallisuustasoltaan 313 bitin elliptisenkäyrän salausta.

$$y^2 = x^3 + ax + b$$



(Kuva 2 , Elliptinen käyrä)

Elliptisen käyrän salausmenetelmän turvallisuus perustuu yksisuuntaisen laskutoimituksen käänteisoperaatioon, tässä tapauksessa diskreetin logarytmin vaikeuteen. Kryptografiassa käytetyt elliptisetkäyrät eivät näytä käyriltä vaan joukolta pisteitä. Pisteiden kertolasku *k***P**, missä kokonaisluku k on määritelty laskemalla piste **P** yhteen itsensä kanssa k-1 kertaa. Tämä on kuitenkin todella hidasta kun *K* on suuri luku. Operaatiota voidaan nopeuttaa laskemalla pisteet pareittain yhteen esim. 16**P** seuraavasti *(Joutsjoki 2019, 9)*

$P_2 = P + P$

$P_4 = P_2 + P_2$

$P_8 = P_4 + P_4$

$P_{16} = P_8 + P_8$

Elliptisenkäyrien avulla toteutettu avaimien vaihtaminen toteutuu seuraavasti :

Q = kP mod p.

Kokonaisluku k on osapuolen A yksityinen avain ja Q julkinen avain.
Järjestelmä perustuu siihen oletukseen, että pisteestä Q salaisen k arvon päätteleminen on vaikea ongelma. Elliptisen käyrän salausmenetelmä on alkanut hiljalleen syrjäyttämään sen edeltäjäänsä RSA:ta. Elliptisen käyrän salausta kuitenkin uhkaa kvanttitietokoneiden ja niiden laskentatehon kehittyminen. *(Joutsjoki 2019, 9-10)*

Monet kryptovaluutat turvautuvat ECDSA:n (Elliptic Curve Digital Signature Algorithm) Mutta ECDSA on helposti murrettavissa Shorin kvanttimatemaattisen algoritmin variaatiolla. Elliptisen käyrän salauksella salatut viestit ovat purettavissa Shorin algoritmillä ja kvanttitietokonetta voidaan tehokkaasti hyödyntää yksityisen avaimen löytämiseen julkisesta avaimesta.
(Tessler and Byrnes, 3)

Julkinen avain tosin paljastetaan yleensä vain silloin, kun transaktio on tapahtumassa ja jokaiselle transaktiolle luodaan oma julkinen avaimensa (bitcoin protokolla).
Transaktion toteutuminen voi Bitcoinin tapauksessa kestää kymmenestä minuutista tuntiin ja tätä aikaikkunaa voidaan hyödyntää kvanttihyökkäyksessä. 256 bittisen ECDSA salauksen purkamiseen on arvioitu tarvittavan n.1500:lla kubitilla toimiva kvanttitietokone. Kvanttitietokoneen täytyisi myös suorittaa operaatioita n. 660MHz nopeudella.
(Tessler and Byrnes, 4)

3.0 KVANTTITIETOKONEET

3.1 Kvanttitietokoneiden perusteet

Kvanttitietokoneet ja niiden laskentakyky perustuu muutamaan kvanttimekaniikkan ilmiöön, kuten superpositioon, lomittumiseen sekä kvantti-interferenssiin. Klassisessa tietokoneessa laskennallisuuden perusyksikkönä on bitti jota voi edustaa tila 0 tai 1. Kvanttitietokoneen bittiä kutsutaan qbitiksi (Quantumbit , kvanttibitti), joka voi olla missä vain tilassa 0 ja 1 välillä kunnes sen tila mitataan. Kvanttibitti voi siis olla kumpikin biteistä samanaikaisesti.

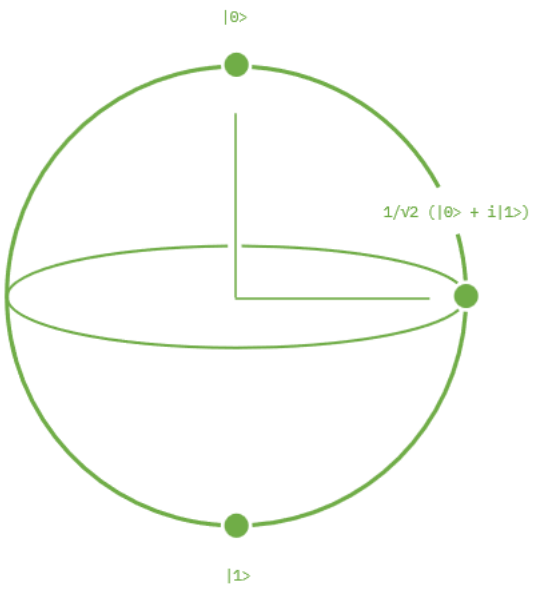


Figure 1: Superposition

(Kuva 3, superpositio)

Kun qbitin tila mitataan se luhistuu klassiseksi tilaksi joko 0 tai 1. Qbitin tilaa ennen mittaamista kutsutaan superpositioksi ja sitä merkitään:
(Joutsjoki 2019, 15)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Lomittuminen (Quantum entanglement) on kvanttimekaaninenilmiö jolle ei ole selitystä

klassisessa mekaniikassa. Yksinkertaisesti selitettynä kaksi hiukkasta ovat relaatiossa toisiinsa vaikka olisivat kaukana toisistaan.
Kun hiukkanen$_1$ mitataan, määrää se myös hiukkasen$_2$ mittaustuloksen. Tämä on mysteerinen ominaisuus, jossa kaksi hiukkasta jakavat olemassaoloansa vaikka ne ovat fyysisesti erillään.

Lomittuminen mahdollistaa sen, että Qbitti voi olla tilassa 1 tai 0 samanaikaisesti kunnes sen tila mitataan.
(Squires E. 1986 , 103)

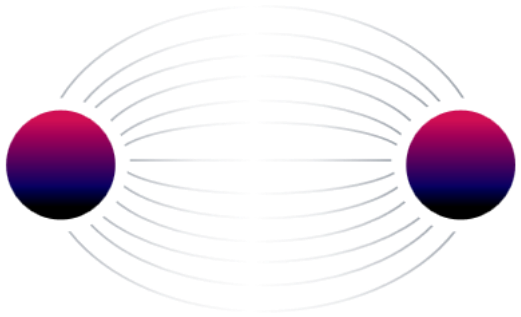


Figure 2:
Entanglement

(Kuva4 lomittuneet partikkelit)

Koska kvanttitietokone on laskentateholtaan paljon edistyksellisempi kuin perinteinen tietokone, se pystyy laskemaan esimerkiksi salausavaimia huomattavasti suuremmalla nopeudella. Koska lohkoketjut toimivat konsensusmekanismilla, tarvitaan lohkoketjun väärentämiseen enemmistö laskentakapasiteetista. Tätä hyökkäystekniikkaa lohkoketjuja vastaan kutsutaan nimellä 51% hyökkäys, jota käsitellään tarkemmin kohdassa 5.2 .

51% hyökkäyksessä taloudellinen hyöty on lohkoketjun louhijoiden puolella, koska louhintaan investoidun laitteiston tuotto-odotus on suurempi, kuin teoreettisen hyökkäyksen tuotto-odotus lohkoketjua vastaan.

Matemaatikko Divesh on vuoden 2017 tutkimuksessaan *”Quantum attacks against bitcoin and how to protect against them”* esittänyt, että lohkoketjuteknologian turvallisuus on

uhattuna, kun kvanttitietokoneet ovat tulevaisuudessa kehittyneet tarpeeksi tehokkaiksi. *(Sanmark 2019, 78)*

3.2 Kvanttitietokoneiden status

John Preskill on määrittellyt kvanttiylemmyyden, jossa kvanttilaskennalliset tietokoneet onnistuvat ratkaisemaan ongelmia, joihin ei klassinen tietokone kykene.
Kryptografian kannalta tämä tapahtuu esimerkiksi silloin, kun Shorin algoritmin avulla voidaan murtaa RSA tai Elliptisenkäyrän salausmenetelmä. Kvanttitietokoneiden rakentaminen on erittäin haastellista, koska kubitteina toimivat erittäin pienet, elektronien tai fotonien kokoiset partikkelit. Jotta superpositiossa olevat kubitit saataisiin vakaiksi vaatii se erittäin stabiilit olosuhteet. Kubittien vakaan superposition saavuttamiseksi kvanttitietokoneen prosessorin täytyy olla jäähdytettynä lähes absoluuttisen nollapisteen tasolle. Kubitin superpositio on myös herkkä erilaisille magneettikentille ja niiden muutoksille.
(Joutsjoki 2019, 31)

Koska kvanttibitit ovat erittäin herkkiä häiriölle on myös kvanttitietokoneiden virheosuus huomattavasti korkeampi kuin klassisella tietokoneella. Kun kubitti häiriintyy, saatta se polarisoitua ykkösestä nollaksi tai nollasta ykköseksi, mitä ilmiötä kutsutaan bitin flippaamiseksi. Kun bitti flippaa, niin algoritmi ja sen ajaminen pysähtyy tuloksetta. Bittien flippaamiseen on kuitenkin esitetty erilaisia monimutkaisia ratkaisuja.

Kubittien superposition herkkyys häiriölle sekä kvanttibittien flippaaminen ovat tämän hetken merkittävin ongelma kvanttitietokoneiden kehitykselle ja toiminnalle.

Google johtaa kvanttitietokoneiden kilpailua tällä hetkellä 72:lla kubitilla (Google Bristlecone) 0.4% virheosuudella.
(Baumhof A.)
IBM:llä on 52 kubitin kvanttitietokone. IBM lainaa kvanttitietokonetta IBM-QUANTUM pilvipalvelussa.
(Giles M. MIT)

4.0 KVANTTIALGORITMIT

Kvanttilaskennan sekä kvantti-informaatiotieteen kehitys katsotaan alkaneen 1980 luvun alussa. Klassisessa matematiikassa yksi tapa mallintaa laskentaa ovat kaaviot loogisista porteista koostuvista piireistä. Kvanttimatematiikassa voidaan myös mallintaa kvanttilaskentaa kvanttiporteista koostuvilla kvanttipiireillä. Kvanttilaskennalla voidaan tehdä samoja laskennallisuuksia kuin klassisella matematiikalla ja vähintääkin yhtä tehokkaasti.
(Katajisto 2015, 1)

4.1 Shorin kvanttialgoritmi

Shorin algoritmi nimettiin matemaatikko Peter Shorin mukaan ja se on kvanttialgoritmi suurten kokonaislukujen tekijöihin jakoa varten. Algoritmi keksittiin vuonna 1994 AT&T-yhtiön Bell Labsissa New Jerseyssä, jolloin Peter Shor osoitti, kuinka kvanttitietokone laskee erittäin suurten lukujen tekijät todella nopeasti.
(Brown , 25)

Shorin algoritmi voidaan jakaa kahteen osaan, klassiseen-, sekä kvanttiosaan. Klassinen osa suorittaa lukujen valintaa ja varmistaa, että valitut luvut ovat sopivia algoritmiin. Kvanttiosassa tapahtuu kvanttilaskeminen modulaarista aritmetiikkaa sekä kvanttibittien superpositiota hyödyntäen.
(Enckell 2019, 1)

Suurten kokonaislukujen alkutekijöihin jako on niin vaikea matemaattinen ongelma, että monet laajasti käytetyt kryptofrafiset salaukset perustuvat tämän ongelman vaikeuteen. Tehokkaimpanakin tunnetun klassisen algoritmin laskemiseen kuluva aika *t* kasvaa lähes eksponentaalisesti kokoaisluvun kasvaessa. Koska Shorin algoritmi hidastuu sen sijaan vain polynomiaalisesti voitaisiin sillä saavuttaa laskennassa lähes eksponentiaalinen nopeuden kasvu.
(Honkanen 2021, 17)

4.2 Groverin etsintäongelman kvanttialgoritmi

Groverin algoritmi on Lov Groverin kehittämä kvanttilaskentaan perustuva algoritmi Shorin algoritmin tapaan se keksittiin myös Bell Labsissa mutta jo vuonna 1996.

Tiedon hakeminen jäsentämättömän datan tietokannasta, on yleinen laskennallinen ongelma tietojenkäsittelytieteessä. Groverin algoritmi suoriutuu jäsentämättömän datan etsintäongelmasta merkittävästi nopeammin, kuin yksikään klassinen algoritmi.
Vaikka Grover alunperin esitteli hakualgoritminsa suurten tietokantojen hakuongelmaan, ei sen kirjaimellinen käyttö tietokantahakuihin ole realistinen.

Groverin algoritmin ajamiseksi olisi tiedon oltava tallennettuna kvanttibittien superpositiotiloihin. Tiedon pitkäaikainen säilyttäminen kvanttibiteissä ei kuitenkaan ole mahdollista, koska kvanttibitit ovat erittäin herkkiä erilaisille häiriöille. Tietokantahakutehtävien sijaan Groverin algoritmi voisi kuitenkin haastaa klassiset algoritmit kryptografisten avainten etsinnässä.
(Honkkanen 2021,19)

5.0 PERUSTASON HYÖKKÄYKSET

Kryptovaluutoilla on useita tunnettuja haavoittuvuuksia, joiden hyväksikäyttö voi johtaa suuriin taloudellisiin menetyksiin tai palveluiden estymisiin. Yleisimmät kryptovaluuttojen suojauksiin kohdistuvat uhat ovat 51 % hyökkäys, DDOS-hyökkäys (Distributed denial of service), Epsilon-hyökkäys, BGP-hyökkäys (Border Gateway Protocol), Long-Range-hyökkäys sekä Sybil-hyökkäys.

Kun kvanttitietokoneiden laskentateho ja toimintavarmuus kehittyvät voidaan niiden laskentatehoa teoriassa hyödyntää hyökkäämään kryptovaluuttoja ja niiden lohkoketjua louhivaa solmuverkostoa vastaan.

5.1 Double-Spending eli kryptovaluutan uudelleenkäyttö exploitaatio

Vaikka kryptovaluuttojen lohkoketjuja vastaan voidaan hyökätä monilla erilaisilla tekniikoilla, lähes jokaisen kryptovaluuttoihin kohdistuvan hyökkäyksen päätavoitteena on kryptovaluutan uudelleenkäyttö *l.* exploitaatio.

Kryptovaluutan uudelleenkäytön *l.* exploitaation tarkoituksena on huijata lohkoketjuverkkoa niin, että ketjussa jo käytettyjä varoja ei olisikaan koskaan käytetty. Uudelleenkäytön mahdollistaminen vaatii sen, että hyökkääjä, jolla on kryptovaluuttaa on käyttänyt kryptovaluuttansa virallisessa ketjussa. Sen jälkeen hyökkääjä rakentaa salassa muilta, uutta pidempää ketjua, jossa varoja ei ole koskaan käytetty. Kun ketju jossa varoja ei ole käytetty on tarpeeksi pitkä, esittelee hyökkääjä sen muille lohkoketjuverkoston solmuille. Koska hyökkääjän salassa rakentama ketju on pidempi, hyväksyy verkosto sen ja hylkää ne lohkot ketjusta, joissa hyökkääjän varat olivat jo käytetty.

5.2 51% hyökkäys

51% hyökkäystekniikka perustuu siihen, että hyökkääjä saa suurimman osan verkon tarkistelaskentatehosta haltuunsa huijatakseen muita verkon solmuja ja konsensusmenetelmää. Hyökkäys alkaa siten, että hyökkääjä laskelmoi osan lohkoketjusta salassa muilta verkon solmuilta ja myöhemmin esittää ennalta laskemansa valheellisen osan ketjua muille verkoston solmuille.

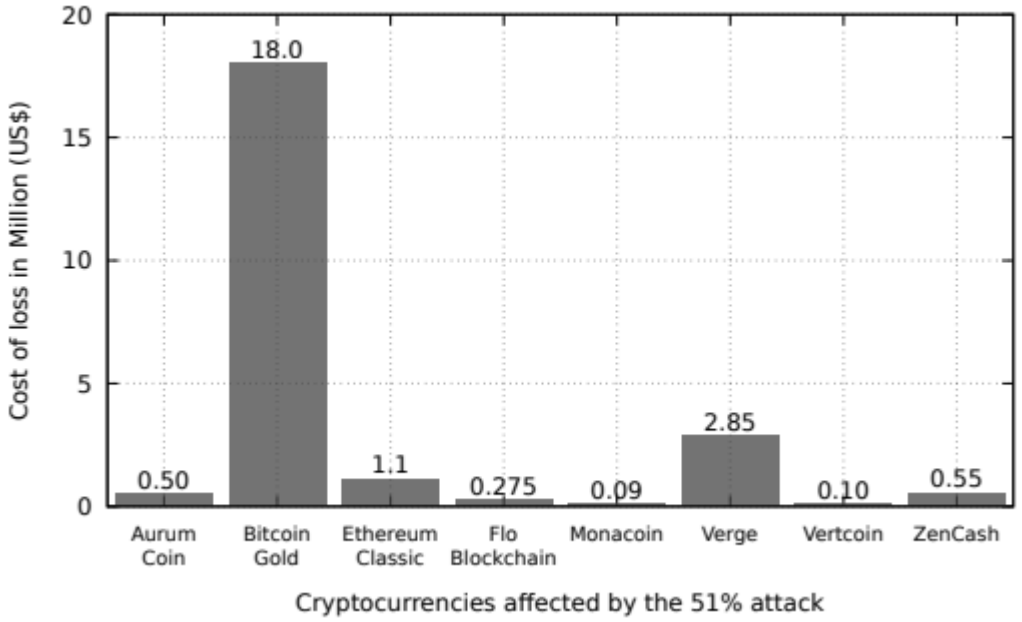
Kun hyökkääjä on saanut suurimman osan verkon laskentatehosta haltuunsa (51%) voi hän pakottaa muut seuraamaan hänen ennalta luomaansa ketjua, mikä mahdollistaa käytännössä kryptovaluutta varojen uudelleenkäyttön *l.* exploitaation (double-spending).

Koska lohkoketju toimii käytännössä niin, että pisin ketjunosa määrää mitä polkua lohkoketju seuraa, hyökkäykselle ei ole välttämätöntä se, että hyökkääjä saa puolet verkon laskenta tehosta, mutta se tekee hyökkäyksen onnistumisesta todennäköisempää.

Mitä enemmän tarkisteen laskentatehoa lohkoketjuverkolla on yhteensä, sitä kalliimmaksi hyökkäys sitä vastaan tulee. Täten mitä korkeampi laskentateho lohkoketjuverkolla on, sitä turvallisempi se on 51% hyökkäystä vastaan.
(Sayeed 2019, 4-5)

Kvanttitietokoneen laskentateho ei ole SHA-256 tarkisteen laskentaan erityisen tehokas eikä se ylitä $2^{256} / T$

Koska SHA-256 tarkisteen purkamiseen ei ole vielä löydetty klassista- tai kvanttialgoritmiä, eivät kvanttitietokoneet ole vielä erityisen tehokkaita bitcoinin louhimiseen tai 51% hyökkäyksen toteuttamiseen. SHA-256 tarkisteen käänteistä laskemista eli purkamista ei ole kuitenkaan todistettu matemaattiseksi mahdottomuudeksi.
(Louis Tessler & Tim Byrnes)



(Kuva 5, kryptovaluutat ja 51% hyökkäys)

Kuvassa esitetty kryptovaluuttojen lohkoketjuihin kohdistettujen 51% hyökkäysten saavuttama rikoshyöty eräänä ajanjaksona.
(Sayeed 2019, 4-5)

5.3 DDOS- hyökkäys

Distributed denial of service hyökkäys eli DDOS. DDOS- hyökkäyksen kohteeksi valittua palvelua tai verkkoa häiritään kohdentamalla siihen suuria määriä ylimääräistä liikennettä. DDOS hyökkäykset vaativat hyökkääjältä bottiverkon tai suuren määrän tietokoneita toteuttamaan suuren määrän palvelupyyntöjä hyökkäyksen kohteena olevaan palveluun. DDOS hyökkäys on tunnettu jo ainakin kahden vuosikymmenen ajan.

Tutkimustieto indikoi, että DDOS hyökkäyksien määrä ja tehokkuus on kasvussa. Keskimäärin DDOS hyökkäyksen rikoshyöty oli 2milj.US$ per hyökkäys vuonna 2018.

DDOS hyökkäys on yleisimpiä hyökkäysmuotoja lohkoketjuverkostoja vastaan. Niiden tarkoituksena yleensä on estää autenttisia transaktioita tapahtumasta ja korvata niitä tekaistuilla transaktioilla. Lohkoketjuverkon hajautetun rakenteen vuoksi, verkkoa pystytään häiritsemään vain rajoitetulla kapasiteetilla.
(Sayeed 2019, 5)

5.4 BGP-hyökkäys

Border gateway protocol (BGP) hyökkäys tunnetaan myös verkon reitityshyökkäyksenä. BGP-hyökkäys harhauttaa internetpalvelun tarjoajaa lähettämään tietoliikennettä väärää reittiä lohkoketjuverkossa ja hyökkäyksen tavoitteena on double spending exploitaation mahdollistaminen.
(Sayeed 2019, 6)

BGP-hyökkäyksiä voidaan toteuttaa erilaisilla tavoilla erilaisiin hyökkäystarkoituksiin. BGP-hyökkääjä voi ilmoittaa jonkun toisen tahon käytössä olevan IP-osoitteen reitti-ilmoituksenaan internetpalvelun tarjoajalle. Mikäli reitti hyökkääjän osoitteeseen on lyhempi, reitittää internetpalvelun tarjoaja tietoliikenteen hyökkääjän osoitteeseen. Hyökkääjä voi uudelleenohjata tietoliikenteen salakuuntelemisen sekä mahdollisen tiedon tallentamisen jälkeen alkuperäiseen oikeaan osoitteeseen, jolloin tieto saavuttaa alkuperäisen osoitteen, mutta pienellä viiveellä. Tässä tapauksessa hyökkäystä on vaikea tunnistaa. On myös mahdollista, että hyökkääjä ilmoittaa internetpalvelun tarjoajalle tarkemman osoitteen, jolloin kaikki tietolliikenne reitin pituudesta huolimatta lähetetään hyökkääjän osoitteeseen.
(Jussila 2020, 3-4)

BGP:ssä ei ole protokollan sisäistä tietoturvaa, jonka avulla reitti-ilmoituksen lähettäjän henkilöllisyys voitaisiin varmentaa tai ilmoituksen sisällön autenttisuuden varmentaa. BGP:n tietoturvapuuttellisuus tekee siitä altistuvaisen niin tarkoituksellisille hyökkääjän kaappauksille sekä myös inhimillisille näppäilyvirheille, jonka seurauksena internet reitityksen turvallisuus saattaa vaarantua.
(Jussila 2020, 1)

Suurin osa bitcoin lohkoketjuverkon solmuista ja niiden toiminnasta kuuluu muutaman internetpalvelun tarjoajan alaisuuteen. Kolmetoista internetpalvelun tarjoajaa kattaa n. 30% koko bitcoin lohkoketju verkoston yhteyksistä.
(ETH- Zurich)

5.5 Sybil- hyökkäys

Sybil- hyökkäyksen tarkoituksena on korruptoida lohkoketjun P2P-verkosto (peer to peer) luomalla useita tekaistuja identiteettejä. Hyökkäyksen tekijät luovat verkkoon useita solmuja (node), jotka vaikuttavat autenttisilta , mutta ovat väärennettyjä.

Nämä väärennetyt solmuidentiteetit korruptoivat verkkoa validoimalla valtuuttamattomia transaktiota ja muuttamalla valideja transaktioita.

Hyökkääjä voi käyttää useita eri laitteita, virtuaalikoneita tai IP-osoitteita verkon valesolmuina. P2P- lohkoketjuverkko olettaa, että yhdellä solmulla olisi myös yksi identiteetti. Hyökkääjän hallitsemat useat solmut jotka toimivat valeinditeetillä voivat kuitenkin lohkoketjuverkossa kiistää lohkojen autenttisuuden ja äänestää rehellisiä solmuja vastaan.
(Sayeed 2019, 11)

6.0 KRYPTOVALUUTTOJEN TEOREETTISET KVANTTIUHAT

Kvanttiuhat kryptovaluutoille kattaa käytännössä kaksi erilaista algoritmiluokitusta. subgroup-finding algorithms (haku-algoritmi) sekä amplitude amplification algoritmit. Ensimmäiseen algoritmiluokkaan kuuluu Groverin haku-algoritmi, jota käsiteltiin kappaleessa 4.2. Toiseen algoritmiluokitukseen kuuluu Shorin algoritmi, jonka avulla pystytään faktoroida valtavia kokonaislukuja, sekä ratkaista diskreetin logaritmin ongelmaa. Kvanttialgoritmeja on käsitelty tarkemmin kappaleessa 4.0

6.1 Laskentateho

Ymmärtäkseemme kvanttitietokoneen laskentatehoa paremmin, voimme hakea perspektiiviä klassisen tietokoneen kyvystä murtaa 2048bit RSA salaus 5GhZ prosessoritaajuudella. Tämän laskentatehtävän teoreettinen suorittaminen kestäisi n. 13.7 miljardia vuotta. Samaisen RSA salauksen purkaminen kvanttitietokonella on arvioitu kestävän kestävän vain 42 minuuttia. Tehokkaasti toimivan kvanttitietokoneen arvioiduksi valmistumis-, ja käyttöönottovuodeksi on arvioitu vuotta 2035.
(Kearney & Perez Delgado, 2)

6.2 Muunnelmat

Toinen kvanttialgoritmiluokka perustuu Groverin algoritmin erilaisiin muunnelmiin. Groverin algoritmillä toteutetussa hyökkäyksessä groverin algoritmiä käytettäisiin suorittamaan (PoW) eli luomaan uutta kryptovaluuttaa kvanttilaskentatehoa hyödyntäen.

Groverin algoritmiä hyödyntämällä voidaan siis teoriassa toteuttaa 51% konsensus-hyökkäys, koska sillä saavutettava laskentateho ylittäisi puolet kryptovaluuttaverkon laskentatehosta. Groverin algoritmin hyöty verrattuna Shorin algoritmin saavuttamaan hyötyyn on varsin minimaalinen.

7.0 KATSAUS KRYPTOVALUUTTOJEN KVANTTITURVALLISUUTEEN

Lohkoketjuteknologiaa voi kutsua jo verrattain vanhaksi teknologiaksi, sillä se on ollut olemassa jo yli 10 vuotta. Lohkoketjuteknologian turvallisuus kuitenkin perustuu vielä vanhempiin salausprotokolliin. Lähes kaikki virtuaalivaluutta lohkoketjujärjestelmät (bitcoin, ethereum, EC-20 valuutat), lompakko-osoitteet sekä bittitilit ovat suojattu vanhanaikaisilla, kymmeniä vuosia vanhoilla menetelmillä. Yleisin näistä vanhoista menetelmistä on elliptisenkäyrän salausmenetelmä. Vaikka elliptisenkäyrän salausmenetelmän purkaminen on käytännössä mahdoton tehtävä klassiselle tietokoneelle, on se tulevaisuuden kvanttitietokoneen ensimmäisiä kehitystavoitteita. *(Zweil 2018, 10)*

7.1 PQCRYPTO

Vaikka kilpailu kvanttitietokoneiden valtaannoususta on kovassa vauhdissa on myös niiltä suojautumiseen varauduttu hyvissä ajoin monen eri toimijan taholta.
Monien maiden sisäisten turvallisuustoimijoiden , pankkiteollisuuden sekä Euroopan unionin rahoittama PQCRYPTO-ryhmä kehittelee uusia salausprotokollia ja algoritmejä kvanttitietokoneilta suojautumista varten.

PQCRYPTO-ryhmän “ICT-645622” dokumentaatiosta on tullut referenssistandardi kvanttivarmojen salausmenetelmien kehityksessä. “ICT-645622” dokumentaatio suosittelee useampia erilaisia kvanttivarmoja salausmenetelmiä, perustuen tämän hetkiseen kvanttitietokoneiden teoreettiseen tehoon, sekä niiden ennustettuun tulevaisuuteen. *(Zweil 2018,10)*

IBM:n tutkimuksen mukaan “Kvanttitietokoneet ovat tänä päivänä tutkijoiden pelikenttä. Viidessä vuodessa ne ovat valtavirtaa. Viidessä vuodessa kvanttitietokoneiden vaikutukset kantautuvat tutkimuslaboratorioiden ulkopuolelle”.

Kryptovaluuttojen tulisi kehittää kvanttiresistanttisuuttaan bruteforce-hyökkäyksiä vastaan. Kryptovaluuttojen transaktiot perustuvat matemaattiseen ongelmaan, jonka kvanttitietokoneet voivat eksponentiaalisesti nopeamalla laskentatehollaan suorittaa jopa 100 miljoonaa kertaa nopeammin.
(Distributed Ledger Technologies for M2M Communications 2019, 305)

Vaikka kvanttitietokoneeet uhkaavat vahvasti kryptovaluuttojen tulevaisuutta on olemassa jo kryptovaluuttojen edelläkävijöitä, jotka ovat valmistautuneet tai ratkaisseet tulevaisuuden suojausongelmia.

7.2 Riskievaluaatio

Alla olevassa taulukossa on riskievaluaatio taulukko yleisten kryptovaluuttojen suojautumispotentiaalista kvanttihyökkäyksiä vastaan.Taulukko on lainattu Joseph. J Kearneyn sekä Carlos A. Perez-Delgadon tutkimuksesta ”Vulnerabilities of blockchain technologies to quantum attacks”. Alkuperäiseen taulukkoon on lisätty Quantum Resistant Ledger (QRL) sekä mochimo jotka ovat jo esittäneet sekä implementoineet suojauksia kvanttihyökkäyksiä vastaan. Näistä lisää kohdasta 9.0 eteenpäin.

Lohkoketju	Shorin algoritmi	Groverin algoritmi
Bitcoin	X	-
Ethereum	X	-
Litecoin	X	-
Monero	X	-
Mochimo	S	-
QRL	S	-

(kuva 6, riskitaulukko)

X, on altis hyökkäykselle.
S, on suojassa hyökkäykseltä.
-, ei ole varmaa tietoa.

7.3 HTTP ja HTTPS

Kommunikaatio ja datan lähettäminen internetissä tapahtuu pitkälti HTTP ja HTTPS protokollien välityksellä. HTTPS on suojattu SSL/TLS protokollilla.
(Inter American Development bank Quantum Resistance in the blockchain)

SSL/TLS on suojausmenetelmä joka luo sessiolle kertaluontoisen avaimen.
SSL/TLS avainta käyetään tietyn ajanjakson eli session aikana datan kryptaamiseen ja dekryptaamiseen. Kun kaksi osapuolta vastaanottavat sekä lähettävät toisillensa dataa internetissä, käytetään siihen yleensä SSL/TLS suojausta. *(Cloudflare)*

TLS jonka kertaluontoiset avaimet eivät ole kvanttisuojattuja hyödyntävät suojaus-algoritmeja kuten RSA, DH, ECDH, ECDSA ja DSA. Tämä tarkoittaa sitä, että kaikki useimpien lohkoketjun internetkommunikaatio, transaktiot sekä eri solmujen välillä lähetetyt viestit eivät ole kvanttisuojattuja. *(Inter American Development bank 2021, 7)*

8.0 YLEISIMIPIEN KRYPTOVALUUTTOJEN RISKILUOKITUKSET

8.1 Bitcoin

Riskiluokitus : korkea.
Hyökkäyksen kohde: Verkolle julistetut keskeneräiset transaktiot.

Bitcoinin suurin haavoittuvuus on pitkäkestoinen transaktioaika. Koska transaktiot kestävät kauan on aikaikkuna hyökkäykselle suotuisa. Kun transaktiota ei ole vielä kirjoitettu lohkoon mutta se on julistettu, voi hyökkääjä selvittää julkisesta avaimesta transaktion tekijän yksityisen avaimen. Tällä tavoin hyökkääjä voi duplikoida transaktion ja ohjata sen haluaamansa lokaatioon.
(Kearney & Perez-Delgado, 4)

Bitcoin turvautuu elliptisiin käyriin (ECDSA) varmistaakseen, että transaktioita voivat tehdä vain oikeat omistajat. Kuten jo tiedämmäe ECDSA on Shorin algoritmin variaatiolla heikko kvanttihyökkäykselle. Näin ollen bitcoin protokolla suojautuu generoimalla osoitteet ajamalla julkisen avaimen ensin SHA-256:n läpi sekä sen jälkeen RIPEMD-160 läpi.

Bitcoin transaktiot saattavat olla tunnin tai pidempään odotusaltaassa ennen kuin ne käsitellään. Matemaatikot Proos ja Zalka arvioivat, että 256 bittisen ECDSA salauksen purkamiseen tarvittaisiin 1500 qbittiä sekä 6x10^9 qbit lisäyksiä. Tälläisen hyökkäyksen teoreettinen suorittaminen tunnissa vaatisi kvanttitietokoneelta 660MHz porttioperaatio-nopeutta.
(Tessler & Byrnes, 3)

Bitcoin ja sen kryptografiset suojausjärjestelmät ovat alttiita mahdollisille kvanttitietokone-hyökkäyksille jotka hyödyntää Shorin algoritmiä. Yksi hyökkäyksistä voi tulla kuitenkin Groverin algoritmin suorittamana. Groverin hakualgoritmilla voitaisiin saavuttaa niin iso laskentateho, että se syrjäyttäisi yli puolet bitcoinverkoston laskentatehosta. Bitcoinin pow (proof of work) perustuu verkon osallistujien laskentatehoon.

Kun Groverin algoritmi saavuttaisi yli puolet verkon laskentatehosta voisi teoreettinen hyökkääjä käyttää hyväksi verkoston konsensusmenetelmää, diktatoidakseen ketjun seuraavia lohkoja ja täten toteuttaen 51% hyökkäyksen.
(Kearney & Perez-Delgado, 5)

8.2 Ethereum

Riskiluokitus: korkea.
Hyökkäyksen kohde: julkisten avaimien uudelleenkäyttäminen.

Ethereumin haavoittuvuus piilee tilijärjestelmässä, jossa julkisten avaimien uudelleenkäyttö on yleistä. Hyökkäyksiä voidaan suorittaa käyttäjiä vastaan, jotka ovat aikaisemmin tehneet tililtään transaktioita mutta tilille on jäänyt ethereum valuuttaa. Hyökkääjä voi selvittää lohkossa olevan julkisen avaimen perusteella käyttäjän yksityisen avaimen, käyttäen Shorin algoritmiä. Tämä mahdollistaa autenttisen transaktion tekemisen kaapatuilla avaimilla. Jos käyttäjä on jättänyt Ethereum tilille valuuttaa, se on yksityisenavaimen kaapparin armoilla.
(Kearney & Perez-Delgado, 4)

8.3 Litecoin

Riskiluokitus: korkea.
Hyökkäyksen kohde: Verkolle julistetut keskeneräiset transaktiot.

Litecoinin tekninen toteutus on pitkälti samanlainen kuin bitcoinilla. Täten litecoin jakaa myös samat kvanttihaavoittuvuudet bitcoinin kanssa.
(Kearney, Perez-Delgado, 4)

8.4 Monero

Riskiluokitus: kohtalainen
Hyökkäyksen kohde: Salatut transaktiot sekä verkolle julistetut transaktiot.

Monerossa käytetty digitaalinen allekirjoitusmalli edDSA on haavoittuvainen kvanttihyökkäyksille, koska se suojautuu diskreetin logaritmin ongelmalla. Monero kuitenkin suojautuu kvanttihyökkäyksiltä säilyttämällä käyttäjien anonymiteetin sekä paljastamatta transaktioiden sisältämää valuutan määrää.

Moneron hyödyntämä Bulletproof-protokolla salaa käyttäjien identiteetit sekä transaktion sisältämät summat. Koska transaktion sisältö on salattu on hyökkääjällä oltava onnea, arvoltaan merkittävän transaktion valinnassa. Hyökkääjän valitsema transaktio perustuu sattumanvaraisuuteen.

Moneron hiljattain implementoiman RandomX tekniikan myötä on sen resistanssi 51% hyökkäystä Groverin algoritmiä hyödyntämällä kasvanut.
(Kearney & Perez-Delgado, 4)

9.0 KVANTTIVARMAT KRYPTOVALUUTAT

9.1 Mochimo

Tässä luvussa esittelemme pääpiirteittäin mochimo kryptovaluutan toimintaperiaatteita, sekä minkälaisilla keinoilla mochimo suojautuu kvanttihaavoittuvuuksilta.

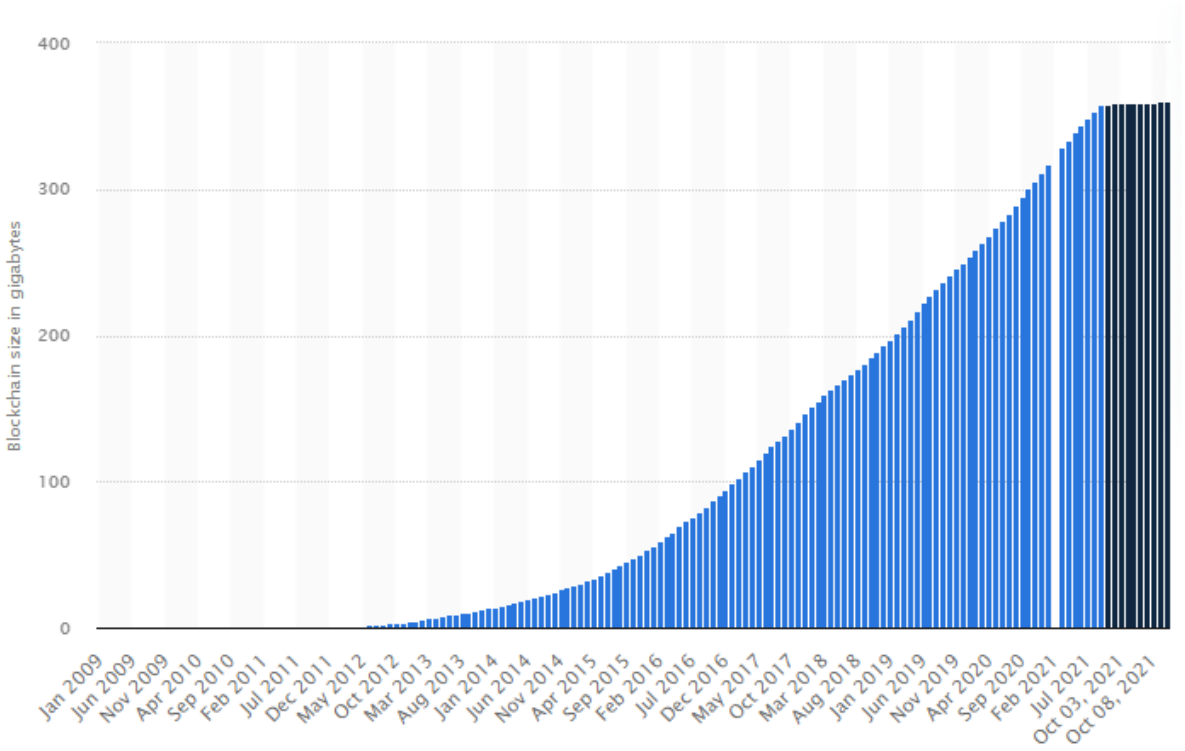
Mochimo-projekti on myös innovoinut useita uusia ideoita, jotka ratkaisevat joitakin kryptovaluuttojen suojaukseen liittyviä pulmia. Mochimon kehittäjät ennustavat, että kvanttitietokoneet rikkoisivat kryptovaluuttojen suojaukset jo vuoteen 2026 mennessä. Mochimon whitepaper:sta käy ilmi, että Mochimon turvallisuuden on vertaisarvioinut Eindhovenin yliopiston matematiikan-, ja tietotekniikanosaston apulaisprofessori Andreas Hulsing. Mochimo käyttää transaktioiden salauksessa seuraavassa kappaleessa kuvailtua eXtended Merkle signature kaava salausta. *(Andreas Hulsingin alkuperäistä vertaisarviointia ei löydy enää internetistä joten sitä ei käsitellä tässä tutkimuksessa)*

9.1.1 Chain Crunch ™ Technology

Mochimo on kehittänyt tekniikan, jolla lohkoketjun lohkoja voidaan arkistoida pienempään tilaan. Tämä tekniikka varmistaa sen, että mochimo skaalautuu lyhyt sekä pitkäaikaisesti. Mochimo skaalautuu yhdestä tuhannesta transaktiosta sekunnissa (TPS) 20 tuhanteen hieman alle seitsemässä vuodessa. Skaalautuvuus on siis mochimonin yksi erityisominaisuus. Chain Crunch-teknologia on yksinoikeudella mochimonin omistuksessa.
(Zweil 2018, 4)

Yksi lohkoketjujen ongelmista on mm. se, että lohkoketjun koko kasvaa koko ajan suuremmaksi, hiljalleen saavuttaen sadat gigabitit tai jopa yhden terabitin. Vaikka bitcoinilla on verrattain pieni osoite ja signatuuri, on se vuoteen 2021 mennessä kasvanut jo 360GB suuruiseksi. Joissakin lohkoketjun sovellutuksissa, mitä suurempi lohkoketju on, sitä kauemmin seuraavan lohkon lisääminen kestää.

Mochimo on ratkaissut kokoon liittyviä ongelmia Chain Crunch ™ teknologiallaan. Käyttäjät pystyvät operoimaan täyttä solmua (full node) pitämällä vain pientä osaa lohkoketjun historiallisesta datasta. Tämä parantaa skaalautuvuutta monella eri tavalla. Verkkoon liittyvän solmun ei tarvitse odotella päiviä tai viikkoja liittymistä vaan voi synkronisoida minuuteissa. *(Zweil ,12)*



(Kuva 7 Bitcoin lohkoketjun koko)

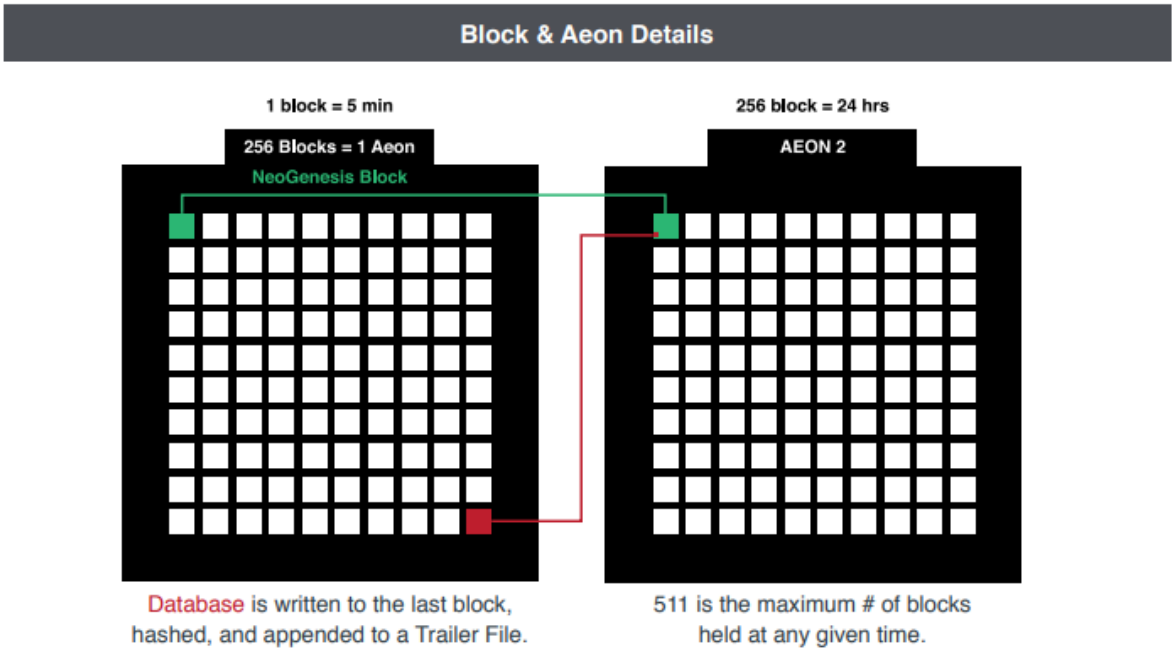
Täyden solmun ylläpitäminen vaatii yleensä koko lohkoketjun säilömistä solmussa, bitcoinin tapauksessa 360GB dataa. Yllä olevassa kuvassa kuvataan bitcoin lohkoketjun kokonaisdatamäärän kehittymistä tammikuusta 2009 - lokakuuhun vuonna 2021.

9.1.2 Chain Crunchin toimintaprosessi

Mochimon yksi ”Aeon” sisältää 256 lohkoa ja sen voi ajatella isompana lohkona tai lohkoperheenä, johon kuuluu useampia lohkoja. Lohkojen välinen ratkaisunopeus eli kuinka usein uusi lohko on generoitu kestää mochimolta 337.5 sekuntia. Tämä antaa yhden Aeonin eliniäksi 86,400 sekuntia (tai yksi päivä).

Mochimo-palvelin sisältää lokaalin tietokannan, joka on indeksoitu lista kaikista mochimoverkon osoitteista, jotka sisältävät mochimo kryptovaluuttaa. Lohkot 1 – 255 ovat varattuja tietokannan eli listan muutoksille ja lisäyksille. Kun mochimo verkossa tapahtuu onnistuneita transaktioita kirjataan ne lohkoihin aina 255 lohkoon saakka.

Kun 255 lohkoa dataa on saavutettu, luodaan koko tietokannasta hajautusfunktio-salattu 256:des lohko, tätä kutsutaan neogenesis-lohkoksi. Neogenesis-lohkon luomisen jälkeen järjestelmä jatkaa lohkon 257 ratkaisemisesta.
(Zweil 2018 , 19)



(kuva 8: ChainCrunch & Neogenesis block)

Kun Neogenesis-lohko on luotu, ei kaikkea historiallista dataa tarvitse enää säilyttää. Tästä syystä mochimo skaalautuu tehokkaasti.

9.1.3 Triggsin algoritmi

Triggsin algoritmi on mochimon omistama ja kehittämä algoritmi, joka takaa FIFO transaktiot (First in first out).

Mochimon Triggs algoritmi takaa FIFO transaktioille kiinteät transaktiokulut, joten mochimo kryptovaluutan louhiminen pysyy kaikentasoisille louhijoille saatavilla.
(Zweil 2018, 4)

9.1.4 Mochimon konsensus

Mochimon konsensus on uudenlainen konsensusmekanismi, joka rakentuu Random Networks -malliin, konvergenssiin, orpojen (hylättyjen) lohkojen karsinnan sekä matemaattisesti todennettavissa olevan konsensukseen. Matemaattisesti todennettavissa oleva konsensus on luotettavampi, kuin monien kryptovaluuttojen hyödyntämä luottamukseen perustuva konsensus.
(Zweil 2018, 4)

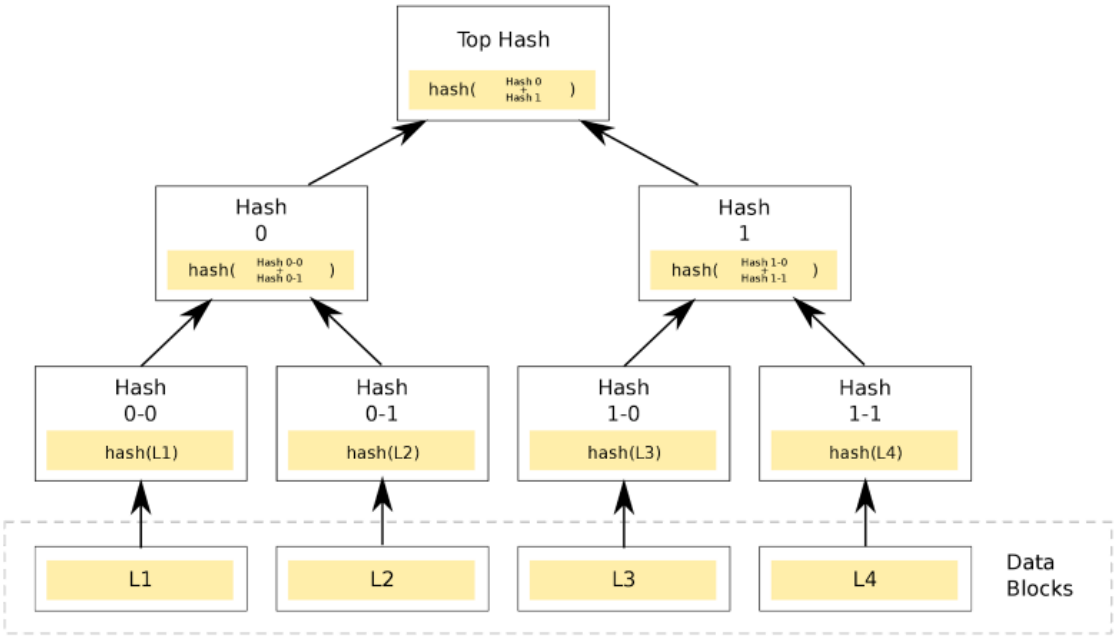
9.2 Quantum resistant ledger (QRL)

Quantum resistant ledger on kansainvälisen tiimin kehittämä kvanttivarma kryptovaluutta. Sen tärkein ominaisuus kryptovaluuttatilikirjana on hajautus-salaukseen perustuvat digitaaliset allekirjoitukset, jotka ovat resistantteja klassisten-, sekä kvanttitietokoneiden hyökkäyksille.

Hajautusfunktioiden generoimiin tarkisteisiin perustuvat digitaaliset-allekirjoitukset ovat kohtalaisen tutkittu aihe ja ne on osoittautunut lupaavimmaksi salausmenetelmäksi kvanttitietokoneiden jälkeiseen aikaan. Siitä syystä hajautusfunktio-salaus on valittu myös QRL:n pääasialliseksi salausmekanismiksi.
(QRL whitepaper, 2)

QRL:n digitaaliset allekirjoitukset ovat salattu käyttäen eXtended **Merkle** Signature -kaavaa eli XMSS:ää. XMSS luo useista kertaluontoisista avaimista (OTS) yhden pitkäaikaisen avaimen. XMSS hyödyntää Winternitz kaavaa, joka generoi 32 satunnaislukua, jotka ovat kaikki 256 bittisiä. Jokainen satunnaisluku salataan hajautusfunktiolla vielä 256 kertaa, SHA-256 salausta hyödyntäen.

Merkle-puuta kutsutaan myös tarkiste-puuksi, mutta ehkä eniten se muistuttaa kuitenkin pyramidia. Ylimpänä puussa on pitkäaikaiseen käyttöön tuleva julkinen avain, joka on luotu hajauttamalla alempien tasojen tarkisteita.
(Marchenkova)



(kuva 9 : Merkle-puu)

OTS avaimet hajautetaan kerran muodostaen puun lehdet(L1-L4), puun lehdet hajautetaan edelleen pareittan yhteen, josta saadaan seuraavan tason tarkiste.

10.0 POHDINTAA

Krpytovaluuttojen kvanttiturvallisuus osoittautui odotettua vaikeammaksi tutkimusaiheeksi rajallisesti saatavilla olevien tutkimusmateriaalien ja niiden osittaisen maksullisuuden vuoksi. Kvanttitietokoneiden laskentateho ja kehittyminen kuitenkin uhkaa yleistä tietoturvallisuutta niin internetin, lohkoketjujen sekä rahatalouden kannalta.

Lohkoketjut sekä niiden mahdollistamat kryptovaluutat ovat vain pieni osa-alue, johon kvanttitietokoneiden tehokuus kohdistuu uhkana. Kvanttitietokoneet ovat teoriassa satoja miljoonia kertoja tehokkaampia kuin klassiset tietokoneet, mutta suurin osa internet-liikenteestä käydään sekä salataan silti klassisilla tietokoneilla. Putoaako internet-, ja maksuliikennesalauksien raskas taakka kvanttitietokoneita vastaan klassisten tietokoneiden harteille, vai turvaudutaanko tulevaisuuden internetin tietoturvallisuudessa myös kvanttietietokoneisiin?

Kvanttitietokoneiden luomat tietoturvauhat ovat kuitenkin tällä hetkellä varsin spekulatiivisia, sillä yhtäkään kvanttitietokonetta ei ole vielä saatu suorittamaan monimutkaisia laskutoimituksia. On kuitenkin selvää, että lohkoketjujen tietoturvallisuus ei ole niin varmaa, kuin kryptovaluuttojen suurimmassa nousuhuumassa on hypetetty.

Kryptovaluuttavarkauksista voi lukea aika ajoin ja rikollisten saavuttama rikoshyöty on usein miljoonia tai kymmeniä miljoonia euroja. Monet argumentoivat myös, että olemassa olevat lohkoketjut voitaisiin helposti ja nopeasti päivittää kvanttiturvallisiksi. Tämä ei kuitenkaan ole mielestäni skaalautuvuuden sekä lohkoketjujen toiminnallisuuden kannalta uskottavaa. Vaikka on jo olemassa paljonkin salausmenetemiä, jotka suojaavat teoreettisilta kvanttiuhilta, ovat ne huomattavasti raskaampia klassisille tietokoneille, kuin tällä hetkellä lohkoketjuja suojaavat algoritmit.

Näyttäisi kuitenkin siltä, että olemassa olevilla kvanttivarmoilla kryptovaluutoilla on merkittävää tulevaisuuspotentiaalia, vaikka niiden olemassaolosta vielä harvat tietävät. QRL on kuitenkin saanut jonkun verran kannatusta sijoittajien keskuudessa ja sen arvo noteerattuna on jo 0.2$ / kpl.

Kryptovaluuttoja on lukematon määrä ja uusia syntyy ja kuolee lähes päivittäin. Vuoden 2021 helmikuussa muutamat eri lähteet uutisoivat Capital Corp Merchant Bankingin kosiskelleen erästä Unkarilaista kvanttisuojattua kryptoprojektia 173 miljoonan dollarin investoinnilla.

Voidaan siis todeta, että kvanttivarmat kryptovaluutat ovat myös sijoittajien mielestä arvokas tulevaisuuden sijoituskohde. Uusien kryptovaluuttojen on kuitenkin vaikea haastaa tunnettuja ja vakiintuneita kryptovaluuttoja, joiden arvoa ylläpitää ns. ”First movers advantage”.

Vaikka uusien kryptovaluuttojen käytännöllisyys sekä tulevaisuuden potentiaalit olisivat parempia, kuin nykyisten tunnettujen valuuttojen, ne eivät saavuta tunnettuutta eivätkä siten pääse näyttämään potentiaaliaan. Kvanttiturvallisia kryptovaluuttoja onkin markkinoilla todella vähän verrattuna kryptovaluuttojen kokonaismäärään, vain muutama itseasiassa.

Koska lohkoketjujen haavoittuvaisuuksia tunnetaan jo kohtalaisen hyvin, voidaan niiden kautta ja niiden avulla varautua tulevaisuuden uhkiin, joita kvanttitietokoneet tuovat tullessaan. Teeoriat haavoittuvuuksista eivät sellaisenaan muutu, mutta kun kvanttitietokoneiden käytännön implementaatiot realisoituvat, löydetään uusia ja ennalta tuntemattomia haavoittuvaisuuksia.

Lähteet:

Baumhof, A. 2019. Breaking RSA Encryption
Luettavissa: https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/
Luettu : 10.10.21

Tessler, L. & Byrnes, T. 2017. Bitcoin and quantum computing

Brown, J. 2001. *Kvanttitietokone*. Terra Cognita,

Bult, T. 2019. Security analysis of blockchain technology. Luettavissa: www.theseus.fi/bitstream/handle/10024/169305/Security%20analysis%20of%20blockchain%20technology.pdf

Cloudflare, What is a Session key? Luettavissa: www.cloudflare.com/learning/ssl/what-is-a-session-key/ Luettu: 20.10.2021

Zivic, N., Ruland, C., Sassmannshausen, J. 2019. Distributed Ledger Technologies for M2M Communications
Luettavissa: siegen.de/dcs/icoin_2019.pdf

Enckell, A. 2019 , Shorin Algoritmi
Luettavissa: http://www.courses.physics.helsinki.fi/fys/lukseminaari/kooste-enckell-hl.pdf
Luettu 30.11.21

ETH-Zurich, Blockchain meets internetrouting
Luettavissa: https://btc-hijack.ethz.ch/ Luettu : 10.7.2021

Giles, M. MIT 2021
IBM's New Qbit Quantum Computer is The Most Powerful Machine You Can Use
Luettavissa: www.technologyreview.com/2019/09/18/132956/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/
Luettu: 18.10.21

Heino, E., Kaskinen, N., Kinnunen, S., Väinämö, S. 2018 *Kryptovaluutat ja lohko-ketjuteknologia. Helsingin yliopisto.*

Honkanen, E. 2021. Kvanttilaskenta,
Luettavissa: https://trepo.tuni.fi/bitstream/handle/10024/132310/HonkanenEetu.pdf

Hyppänen, A. Bitcoinkeskus. luettavissa: https://bitcoinkeskus.com/alysopimus-smart-contract/
Luettu : 4.6.21

Marcos, A., López, D., Cerón, S., Leal, A., Pareja, A., Da Silva, M., Pardo, A., Jones, D. Worrall, D., Merriman, B., Gilmore, J., Kitchener, N., Venegas, S. , Andraca.
Inter American Development bank Quantum Resistance in the blockchain 2021
Luetavissa: https://publications.iadb.org/publications/english/document/Quantum-Resistance-in-Blockchain-Networks.pdf
Luettu: 9.10.21

Joutsjoki, S. 2019. Kvanttitietokoneiden vaikutus kryptografiaan.
Luettavissa: https://trepo.tuni.fi/bitstream/handle/10024/116145/JoutsijokiSami.pdf

Jussila, H. 2020. Tekniikat internet-reititysten kaappaamisen estämiseksi
Luettavissa:
https://jyx.jyu.fi/bitstream/handle/123456789/68916/URN%3aNBN%3afi%3ajyu-202005113122.pdf
Luettu: 20.6.2021

Karhunen, S. 2018. Lohkoketju ja älykkäät sopimukset s. 9
Luettavissa:
https://www.theseus.fi/bitstream/handle/10024/143185/Karhunen_Sami_2018_04_13.pdf
Luettu: 4.5.21

Katajisto, V. 2015. Kvanttilaskenta ja Shorin algoritmi.
Luettavissa: http://www.courses.physics.helsinki.fi/fys/lukseminaari/kl2015/katajisto-kooste.pdf Luettu: 30.11.21

Marchenkova, A. Are these cryptocurrencies quantum secure?
Luettavissa: https://www.amarchenkova.com/posts/quantum-secure-cryptocurrencies-qrl-mochimo-iota-cardano
Luettu: 3.11.21

Northcrypto. Mikä on lohkoketju? Luettavissa: www.northcrypto.com/fi/about/blockchain
Luettu: 18.8.21

QRL Abstract.
Luettavissa: https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf
Luettu: 10.11.21

Sayeed, S., 2019. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack

Squires, E., 1986. The Mystery of the Quantum World

Virtuaalivaluutta Mikä on lohkoketju eli blockchain *Luettavissa: www.virtuaali-valuutta.com/lohkoketjuteknologia*

Kearney, J. &.Perez-Delgado, C. 2021. Vulnerabilities of blockchain technologies to quantum attacks.
Luettavissa:
https://www.sciencedirect.com/science/article/pii/S2590005621000138?via%3Dihub
Luettu: 15.8.21

Zweil, M. 2018. Mochimo Post-Quantum currency white paper. Luettavissa:
https://mochimo.org/wp-content/uploads/dlm_uploads/2018/04/mochimo_wp_EN.pdf
Luettu: 28.04.2021

Kuva 1., Visualisointi lohkosta , Heino E, Kaskinen N., Kinnunen S., Väinämö S. Helsingin yliopisto, 2018 *Kryptovaluutat ja lohkoketjuteknologia Helsingin yliopisto.*

Kuva 3., Superpositio (IBM.COM)

Kuva 4., Lomittuneet partikkelit (IBM.COM)

Kuva 5., lohkoketjut ja 51%. Sayeed S. 2019 Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack

Kuva 6., Riskitaulukko. Kearney J. &.Perez-Delgado C. 2021 Vulnerabilities of blockchain technologies to quantum attacks Kearney J. &.Perez-Delgado C.

Kuva 7., Bitcoin lohkoketjun koko. (https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size)

Kuva 8., *ChainCrunch & Neogenesis block.* Zweil, M. 2018. Mochimo Post-Quantum currency white paper.

Kuva 9., Merkle puu. Marchenkova, A. Are these cryptocurrencies quantum secure?