



# Kryptovaluutan turvallisuus osakeyhtiössä

Janne Lohilahti

2023 Laurea



Laurea-ammattikorkeakoulu

## Kryptovaluutan turvallisuus osakeyhtiössä

Janne Lohilahti  
Turvallisuus ja riskienhallinta  
Opinnäytetyö  
Maaliskuu, 2023

Janne Lohilahti

**Kryptovaluutan turvallisuus osakeyhtiössä**

Vuosi

2023

Sivumäärä

69

Opinnäytetyön tavoitteena oli tuottaa kokonaisvaltainen kehittämistyö, joka vastaisi kysymyksen, miten useamman osakkaan osakeyhtiö voisi mahdollisimman turvallisesti käsitellä ja säilyttää kryptovaluuttoja. Työn toimeksiantajana toimi nimeltä mainitsematon pieni kolmen osakkaan osakeyhtiö. Opinnäytetyön tulokset eivät ole kuitenkaan rajattu pelkästään kyseisen yrityksen käyttöön, vaan kirjoitin työtä sellaisella ajatuksella, että mikä tahansa suuri tai pienempi osakeyhtiö voisi poimia haluamiaan toimintatapoja, vinkkejä sekä neuvoja käyttöönsä.

Tämä opinnäytetyö rakentui seuraavien tutkimuskysymysten ympärille: miten voidaan käsitellä ja säilyttää kryptovaluuttoja turvallisesti osakeyhtiössä, jossa on useampi osakas, mitkä ovat hyviä toimintatapoja kryptovaluuttojen käsittelemiselle, jos usean osakkaan osakeyhtiössä osakas menehtyy tai yksityisavain katoaa, sekä millä tavoin osakeyhtiö voisi ansaita tuottoa kryptovaluuttaomistuksilleen tai hyödyntää louhimista. Keräsin ensin tietoa aineistoa, jonka pohjalta tein puolistrukturoituja teemahaastatteluja. Haastateltuina olivat suomalaisia kryptovaluutta-alan asiantuntijoita. Tämän jälkeen vertasin haastattelutuloksia koostamaani tietoperustaan ja tein omat johtopäätökseni siihen, kuinka kryptovaluuttoja kannattaisi käsitellä turvallisesti osakeyhtiössä.

Hyödynsin työssäni kryptovaluuttoihin perustuvaa tietokirjallisuutta, lainsäädäntöä, vero-ohjeita, asiantuntijoiden kirjoittamia verkkojulkaisuja sekä haastattelemani alan asiantuntijoita. Itselläni on laajaa osaamista ja kokemusta kryptovaluutoista. Tätä vasten vertasin kryptovaluuttoihin perustuvaa tietokirjallisuutta, joka lisää tulosten luotettavuutta.

Tämä opinnäytetyö toimii ajankohtaisena oppaana pienyrityksille, jotka ovat harkinneet ottaa käyttöönsä kryptovaluuttoja osana liiketoimintaansa, mutta sitä voi käyttää muutkin yritykset. Tähän voi kuulua muun muassa sijoittaminen, maksujen vastaanottaminen tai louhiminen. Työssäni kävin läpi myös kirjanpidollisia sekä verotuksellisia asioita kirjoitushetken ajantasaista ohjeita hyödyntäen. Opinnäytetyö oli tehty myös ajatellen sellaisia yrityksiä, jotka ovat jo ennestään tekemissä kryptovaluuttojen parissa, mutta jotka haluavat muuttaa käytäntöjään turvallisimmiksi.

Asiasanat: bitcoin, kryptovaluutat, osakeyhtiö, turvallisuus

Janne Lohilahti

**Security of Crypto Currency Assets in a Limited Liability Company**

Year

2023

Pages

69

---

The goal of the thesis was to produce a comprehensive development work that would answer the question of how a limited company with several shareholders could handle and store crypto currencies as safely as possible. The client of the work was an unnamed small limited liability company with three shareholders. However, the results of the thesis are not limited to the use of the company in question, but I wrote the work with the idea that any large or small organisation could pick up the methods of operation, tips, and advice they want for their use.

This thesis was built around the following research questions: how cryptocurrencies can be handled and stored safely in a limited company with several shareholders, what are the good operating procedures for handling cryptocurrencies if a shareholder in a limited company with several shareholders dies or the private key is lost, and how could the limited company earn a return on its cryptocurrency holdings or utilise mining. First, I collected data, based on which I conducted semi-structured thematic interviews. The interviewees were Finnish cryptocurrency experts. After that, I compared the interview results with the database I compiled and made my own conclusions about how cryptocurrencies should be handled securely in a limited company.

In my work, I made use of information literature based on cryptocurrencies, legislation, tax guidelines, online publications written by experts, and the experts in the field I interviewed. I have extensive knowledge and experience with cryptocurrencies. I evaluated the results by comparing my knowledge to the data, which added reliability to the results.

This thesis acts as a current guide for small companies that has considered adopting crypto currencies as part of their business, but it can be used by other companies as well. This may include, among other things, investing, receiving payments or mining. I also went through accounting and taxation matters, using the instructions that were up to date at the time of writing. The thesis was also made considering companies that are already working with crypto currencies but want to change their practices to be more secure.

Keywords: bitcoin, company, cryptocurrency, security

## Sisällys

1	Johdanto.....	7
1.1	Opinnäytetyön aihe ja tavoitteet.....	7
1.2	Opinnäytetyön rajaukset.....	8
1.3	Kryptovaluuttoihin liittyvät käsitteet .....	8
2	Kryptovaluutat ja riskit.....	12
2.1	Bitcoin ja kryptovaluuttojen historia.....	12
2.1.1	Ethereum ja muut kryptovaluutat .....	14
2.1.2	Skaalausratkaisut ja Bitcoinin tulevaisuus .....	15
2.2	Kryptovaluuttojen ja lohkoketjujen turvallisuus .....	16
2.2.1	Salaus .....	17
2.2.2	BIP-39 .....	17
2.2.3	Avainten jakaminen .....	18
2.2.4	Transaktiot .....	21
2.2.5	Yksityisyys .....	22
2.2.6	PoW ja PoS .....	23
2.2.7	51 % -hyökkäys .....	25
2.2.8	Keskitetyt kryptovaluuttapalvelut .....	25
2.2.9	Lompakot .....	29
2.3	Yritysturvallisuus ja riskienhallinta.....	32
2.3.1	Riskienhallinta .....	33
2.3.2	Tietoturva .....	35
2.4	Kirjanpito.....	36
2.5	Verotus .....	37
3	Opinnäytetyön tutkimusmenetelmälliset ratkaisut.....	37
3.1	Haastattelupohjan laatiminen.....	38
3.2	Tutkimusaineiston kerääminen.....	39
3.3	Haastatteluaineiston käsittely ja analysointi .....	41
4	Tulokset .....	42
4.1	Haastatteluiden tulokset .....	42
4.1.1	Käyttötarkoitukset .....	43
4.1.2	Maksujen vastaanottaminen .....	45
4.1.3	Riskit .....	45
4.1.4	Useamman henkilön pääsy kryptovaluuttalompakkoon .....	46
4.1.5	Toimintatavat avainhenkilön menehtyessä tai avainten kadotessa .....	49
4.1.6	Yksityisyys .....	50
4.1.7	Lainapalvelut.....	51

4.1.8	Louhiminen .....	53
4.2	Tulosten yhteenveto .....	54
5	Johtopäätökset ja pohdinta.....	56
5.1	Johtopäätökset .....	56
5.2	Omaa pohdintaa opinnäytetyöstä ja tutkimuksesta .....	58
5.2.1	Opinnäytetyön luotettavuus .....	59
5.2.2	Opinnäytetyön avoimuus ja tietosuoja .....	59
5.2.3	Eettiset kysymykset .....	60
5.2.4	Tutkimuksen hyödyllisyys ja käyttökelpoisuus sekä tutkimuksen aikataulu .....	60
5.3	Tulosten raportointi toimeksiantajalle.....	60
5.4	Loppusanat, jatkotutkimusehdotus ja kiitokset .....	61
	Lähteet.....	62
	Kuviot .....	67
	Taulukot .....	67
	Liitteet .....	68

## 1 Johdanto

Tämä opinnäytetyö on kehittämistyö. Yhteistyökumppanina toimii yritys X Oy. Yrityksen oikeaa nimeä ei mainita tässä opinnäytetyössä sen takia, että tässä opinnäytetyössä esitetään sekä yrityksen olemassa olevia luottamuksellisia käytäntöjä että mahdollisia opinnäytetyön tutkimustulosten tuomia muutoksia, jotka voivat paljastaa salaisia tietoja tai jotka ovat omiaan aiheuttamaan taloudellista vahinkoa toimeksiantajalle joutuessaan julkisiksi. Kryptovaluutat ovat suhteellisen uusi omaisuusluokka, jonka turvallisuus perustuu varmentamiseen, eikä niinkään paljon luottamukseen. Tämän opinnäytetyön tarkoitus on selvittää, millä tavoin yritys X Oy voisi jatkaa kryptovaluuttojen säilyttämistä ja käsittelemistä turvallisesti tulevaisuudessa.

X Oy:n pääasiallinen toimiala on asuntosijoittaminen. Yritys sijoittaa ja säilyttää kuitenkin varoja kryptovaluutoissa tavoitteena saada sijoitetuille varoille ylimääräistä tuottoa ennen tulevia asuntokauppoja luottaen kryptovaluuttojen korkean arvovaihtelun tuomiin mahdollisiin arvonnousuihin. Tällä hetkellä X Oy tekee kauppaa jatkuvina kuukausitalletuksina ja säilyttää kryptovaluuttoja suomalaisessa Coinmotion-palvelussa. Opinnäytetyön tavoitteena on antaa työkaluja yritykselle jatkaa kryptovaluuttoihin sijoittamista ja niiden säilytystä turvallisesti saavuttaakseen strategiset tavoitteensa.

Opinnäytetyössäni käyn läpi tietoperustassa Bitcoinin ja kryptovaluuttojen historiaa, kryptovaluuttojen ja lohkoketjujen turvallisuutta sekä yritysturvallisuuden ja riskienhallinnan perusteita. Tämän jälkeen opinnäytetyöni tutkimusmenetelmällisenä ratkaisuna käytän puolistrukturoitua teemahaastattelua selvittääkseni alan asiantuntijoiden mielipiteitä, keinoja ja vinkkejä kryptovaluuttojen turvallisesta käsittelemisestä, niiden riskeistä sekä erilaisista toimitavoista säilyttää kryptovaluuttoja turvallisesti yrityksen elinkaareissa. Lopuksi käyn läpi johtopäätökset sekä omaa pohdintaa opinnäytetyöstä ja tutkimusmenetelmällisistä ratkaisuista.

### 1.1 Opinnäytetyön aihe ja tavoitteet

Opinnäytetyön tavoitteena on kryptovaluuttojen käsittelyyn ja säilyttämiseen liittyvien toimintamallien kehittäminen turvallisuus huomioiden osakeyhtiössä X. Tutkimuskysymykset ovat seuraavat:

- Miten voidaan käsitellä ja säilyttää kryptovaluuttoja turvallisesti osakeyhtiössä, jossa on useampi osakas?
- Mitkä ovat hyviä toimintatapoja kryptovaluuttojen käsittelemiselle, jos usean osakkaan osakeyhtiössä osakas menehtyy tai yksityisavain katoaa?

- Millä tavoin osakeyhtiö voisi ansaita tuottoa kryptovaluuttaomistuksilleen tai hyödyntää louhimista?

Yritys X Oy käsittelee ja säilyttää jo tälläkin hetkellä kryptovaluuttoja. Opinnäytetyössäni selvitetäänkin muun muassa sitä, onko kryptovaluuttojen säilyttäminen nykyiseen tapaan Coinmotion-palvelussa jatkossakin turvallista, vai onko muita turvallisempia keinoja säilyttää varoja varsinkin kryptovaluuttavarojen kasvaessa.

Käyn myös läpi muun muassa sitä, mitä toimintasuunnitelmia yrityksellä pitäisi olla huomioiden useamman osakkaan pääsyä käsittelemään yrityksen kryptovaluuttavaroja sekä mitä toimintasuunnitelmia yrityksellä pitäisi olla ennakkoon ja sen varalle, että esimerkiksi yksityisavain kadotetaan, se päättyy pahansuovalle taholle tai avainta säilyttävä henkilö menehtyy.

Lisäksi käyn läpi tapoja, millä yritys voisi saada tuottoa kryptovaluuttaomistuksilleen ja tähän liittyen selvitän, onko lainapalvelut varteenotettavia vaihtoehtoa tuoton ansaitsemiselle. Käyn myös läpi millä tavoin yritys voisi hyödyntää kryptovaluuttojen louhimista.

## 1.2 Opinnäytetyön rajaukset

Tässä opinnäytetyössä ei anneta sijoitusvinkkejä tai puhuta kryptovaluutoista sijoitusmuotona muuten kuin osakeyhtiön kannalta oleellisista verotusnäkökulmista. Verotusnäkökulmatkin liittyvät lähinnä vero-ohjeiden ja lakien noudattamiseen. Opinnäytetyössä ei myöskään avata muiden yritysmuotojen kuin osakeyhtiön tai yksityishenkilöiden kannalta kryptovaluuttojen säilyttämistä tai käsittelemistä, vaikka monia tässä työssä käsiteltyjä asioita voidaankin samalla tavalla hyödyntää muissakin yritysmuodoissa kuin osakeyhtiöissä.

Opinnäytetyö on tarkoitettu tueksi X Oy:lle ja yrityksen ei tule tehdä strategisia päätöksiä pelkästään opinnäytetyön perusteella, vaan yrityksen tulisi tehdä myös omat taustatutkimuksensa. Tässä opinnäytetyössä esiteltyjä kolmannen osapuolen palveluja ei ole tutkittu niin tarkasti, että niiden toimintaa voisi pitää täysin luotettavina. Opinnäytetyön aloituksen ja valmistumisen välissä olen myös joutunut poistamaan useamman yrityksen ja palvelun maininnan työstäni muun muassa sen takia, että palvelu on lopettanut toimintansa tai yritys mennyt konkurssiin. Tämä on erinomainen esimerkki kryptovaluutta-alan nopeasta vaihtelusta.

## 1.3 Kryptovaluuttoihin liittyvät käsitteet

**Avoim lähdekoodi** (engl. open source) tarkoittaa lähdekoodin vapaan lukemisen lisäksi sitä, että kukaan ei rajoita ketään osapuolta myymästä tai luovuttamasta ohjelmistoa, vaikka ohjelmistossa olisi käytetty useista eri lähteistä peräisin olevia ohjelmia. Avoimen lähdekoodin ohjelman tulee sisältää lähdekoodin ja ohjelma täytyy sallia lähdekoodinsa jakelu. Avoimen lähdekoodin lisenssi sallii modifikaatiot ohjelmasta sekä myös modifikaatioiden vapaan

jakelun. Lisenssi voi kuitenkin sallia tai edellyttää, että modifioitu ohjelma käyttää eri nimeä tai versiota, kuin alkuperäinen ohjelma. Lisenssi ei saa rajoittaa ketään käyttämästä ohjelmaa esimerkiksi liiketoiminnassa eikä lisenssi saa syrjiä ketään henkilöä tai ryhmää. (Open Source Initiative 2007.)

**BIP** (Bitcoin Improvement Proposal), eli suomeksi parannusehdotus Bitcoinin lähdekoodiin tai rakenteeseen, on ehdotus Bitcoin-yhteisöltä, jolla saataisiin parannettua Bitcoinin käytettävyyttä. Bitcoinin kehittäjien tulee hyväksyä BIP:in, jotta siitä tulisi muokkaus Bitcoin lähdekoodiin. Ne ehdotukset, jotka ovat hyväksytyt, ja lisätty Bitcoinin rakenteeseen jäävät yleensä tietoisuuteen kyseisen BIP:in numerolla. (Karame & Androulaki 2016, 156.) Esimerkiksi BIP-39 (2022) käsittelee muistitekniesten sanojen käyttöönottoa yksityisavainten tai lompakoiden helpommaksi palauttamiskeinoksi. Muilla kryptovaluutoilla on yleensä vastaavanlaiset käytännöt parannusehdotuksille, esimerkiksi Ethereumin vastaava parannusehdotus on EIP (Ethereum Improvement Proposal).

**Chapter 11** on yhdysvaltalainen konkurssimenettely, joka vastaa Suomessa pitkälti yrityssaneerausta. Velallisella pysyy edunvalvojan valtuudet ja velvollisuudet sekä voi jatkaa liiketoimintaa. Velkojat voivat äänestää saneeraussuunnitelmasta ja tuomioistuim voi vahvistaa suunnitelman, jos se täyttää lain vaatimukset ja saa vaaditut äännet. (United States Courts 2023.)

**Deflaatio** on tavaroiden ja palveluiden yleinen hintojen lasku, joka yleensä liittyy rahan tarjonnan supistumiseen. Deflaation aikana valuutan ostovoima kasvaa ajan myötä. Pääsääntöisesti deflaatio hyödyttää kuluttajia, koska he voivat ostaa enemmän palveluita ja tavaroita samalla nimellistulolla ajan mittaan. Deflaatio voi kuitenkin vahingoittaa esimerkiksi lainanottajia, jotka voivat joutua maksamaan velkansa rahalla, joka on arvokkaampi kuin lainaamansa raha. (Investopedia 2022.)

**ECDSA**, eli Elliptic Curve Digital Signature Algorithm, on digitaalinen allekirjoitusjärjestelmä, joka pohjautuu DSA-algoritmiin, mutta omaa elliptisen käyrän salauksen (Karame & Androulaki 2016, 36). ECDSA ottaa syötteenä viestin sekä yksityisen avaimen ja tuottaa niistä allekirjoituksen (Nakov 2018).

**EIP**, eli Ethereum Improvement Proposal, on samanlainen parannusehdotus Ethereumille kuin BIP on Bitcoinille. EIP-parannusehdotukset kuvaavat Ethereum-alustan standardeja, kuten ydinprotokollamäärittelyt, API:t ja älysopimusstandardit. (Ethereum Improvement Proposals 2022.)

**Escrow** on käsite, joka kuvaa sopimusta, jossa kolmas osapuoli pitää omaisuutta tai rahaa kahden muun osapuolen puolesta, jotka ovat suorittamassa tapahtumaa tai transaktiota. Neutraali kolmas osapuoli pitää varat hallussaan, kunnes ostaja ja myyjä ovat molemmat täyttäneet sopimusvaatimukset. Escrow tarjoaa suojan silloin, kun varojen tai tavarain

vastaanottaja ei muuten voi vakuuttua myyjän luotettavuudesta, vähentäen riskiä varojen menettämiselle. (Banton 2022.)

**Fiat-raha** on valtion liikkeelle laskema valuutta, joka ei ole sidottu fyysiseen hyödykkeeseen, kuten kultaan tai hopeaan, vaan sen liikkeelle laskeneeseen hallitukseen tai tahoon. Fiat-rahaman arvo perustuu kysyntään ja tarjontaan, eikä sitä tukevan hyödykkeen arvosta. Useimmat paperivaluutat, kuten euro ja Yhdysvaltojen dollari, ovat fiat-valuuttoja. Fiat-rahaman liikkeelle laskema taho voi valvoa, kuinka paljon rahaa painetaan. Iso vaara fiat-valuutoissa on se, että sen liikkeelle laskema taho voi tulostaa sitä liikaa, mikä johtaa hyperinflaatioon. (Chen 2022a.)

**Hajautettu verkko** (engl. decentralized network) ei ole minkään keskushallinnon valvonnan alla, vaan sen ohjaus on hajautettu käyttäjien kesken. Verkko ei ole riippuvainen yhdestä tai muutamasta palvelimesta, vaan verkkoa ajetaan P2P-periaatteella, jolloin jokaisella käyttäjällä on yhtäläinen valta. Bitcoinin lisäksi myös itse Internet on hajautettu verkko, vaikka tiedot sivustot ja yritykset, kuten Google ja Meta hallitsevatkin suurta osaa liikenteestä. (Deer 2022.)

**Inflaatio** on vastakohta deflaatiolle. Kun deflaatiossa tavaroiden ja palveluiden hinta laskee ostovoiman noustessa, niin inflaatiossa hinnat nousevat ostovoiman laskiessa ajan myötä. Raha menettää ostovoimansa yleensä sen takia, että rahan liikkeellelaskija tulostaa enemmän rahaa, valuutan arvo alenee tai uusi raha lainataan valtion obligaatioita ostamista varten pankeista jälkimarkkinoilta. (Fernando 2022.)

**Konsensus** on keskeinen käsite saksalaisen Jürgen Habermasin teoriassa, jonka mukaan yksimielisyys poliittisissa ja moraalisisissa kysymyksissä voidaan saavuttaa järkeilyn kautta (Pietari-nen 2015). Bitcoinin lähdekoodin muutoksiin vaaditaan käyttäjien yksimielisyyttä, jotta muutokset voidaan kirjata lähdekoodiin (Karame & Androulaki 2016, 156).

**Kryptovaluutta** (engl. crypto currency) tai virtuaalivaluutta tarkoittaa lain virtuaalivaluuttojen tarjoajista (572/2019) 2 § mukaan digitaalisessa muodossa olevaa arvoa, jota keskuspankki tai muu viranomainen ei ole laskenut liikkeelle, joka ei ole laillinen maksuväline, jota henkilö voi käyttää maksuvälineenä ja joka voidaan siirtää, vaihtaa sekä tallentaa sähköisesti.

**KYC** (Know Your Client) tarkoittaa käytännössä asiakkaan tunnistamista rahanpesusäädösten toteuttamiseksi varmistamalla asiakkaan henkilöllisyyden sekä asiakkaan sijoitusosaamisen ja -profiilin. Vaikka kaikkia kryptovaluutta-alustoja ei vaadita tunnistamaan asiakkaitaan, niin useimmat ovat silti ottaneet käyttöönsä KYC-prosessit, koska yleinen konsensus alalla on se, että halutaan estää rikollinen toiminta, kuten esimerkiksi rahanpesu kryptovaluutta-alustoilla. (Chen 2022b.)

**Lohkoketju** (engl. blockchain) on tietokanta, johon luodaan ketjussa uusia lohkoja, joissa on edellisen lohkoketjussa olevan lohkon tarkiste ja uusi sisältö. Lohkoketjun lohkon sisältöä ei pystytä muuttamaan sen jälkeen, kun se on julkaistu lohkoketjussa, tehden lohkoketjusta turvallisen vaihtoehdon keskitetyille tietokannoille. Ensimmäinen toimiva konsepti lohkoketjusta nähtiin, kun Bitcoin-verkko käynnistettiin. (Nakamoto 2008.)

**Merkle-puu** on puuta muistuttava datarakenne, joka koostuu tiivisteistä. Merkle-puu on yksi lohkoketjujen perusperiaatteista ja sitä käytetään lohkoketjussa varmentamaan tiedon oikeellisuutta. Tiivisteitä luodaan Merkle-puussa alhaalta ylöspäin, joissa myöhemmät tiivisteet luodaan yhdistämällä kaksi aikaisempaa tiivistettä. Jäljelle jäävä juuritiiviste kutsutaan Merkle-juureksi. Merkle-puu vaatii parillisen määrän lehtiä, eli tiivisteitä. (Hyytiäinen 2018.)

**Multisig** tarkoittaa moniallekirjoituksellista (engl. multisignature) transaktiota tai lompakkoa, joka vaatii useamman kuin yhden allekirjoituksen, jotta transaktio toteutuisi (Karame & Androulaki 2016, 40).

**Niukkuus** (engl. scarcity) on Wiktionaryn (2022) mukaan ”vallitseva tila, jossa hyödykettä on tarjolla markkinoilla vähemmän kuin sitä kysytään”. Bitcoin on Ammousin (2019, 230-231) mukaan absoluuttisen niukka sekä varmennettavissa oleva digitaalinen esine ja näin ollen ensimmäinen esimerkki digitaalisesta käteisestä.

**OTC** (lyh. over the counter) on yleisesti ottaen kauppa, joka tapahtuu suoraan kahden asianomaisen välillä ilman pörssien valvontaa. OTC-kryptovaluutat ovat enimmäkseen sellaisia, jotka eivät ole listattuna virallisessa pörssissä erilaisista syistä, vaikka OTC-kauppaa tarjoava olisi itsessään pörssi tai välityspalvelu. Yleensä sellaiset tahot, jotka haluavat ostaa tai myydä suuria määriä kryptovaluuttoja ilman suurempaa sääntelyä tai paremmilla ehdoilla, haluavat tehdä OTC-kauppoja. OTC-kaupoilla ei ole myöskään suurta vaikutusta kryptovaluutan hintaan, eli OTC-kaupat sopivat sellaiselle taholle, joka haluaa minimoida kaupan vaikutukset markkinoihin esimerkiksi ostaessa tai myydessä tuhansia bitcoineja kerralla. (Bradley 2019.)

**SHA256** (lyh. Secure Hash Algorithm 256-bit) on yksi yleisimmistä tiedostojen tai tietojen varmentamiseen käytettävistä tiedonkäsittelyalgoritmeista. Se on turvallinen ja nopea algoritmi, joka muodostaa tiedostosta tai tiedosta 256-bittisen tuloksen (tiivistearvon), joka toimii tiedon varmenteena. Tiivistearvo on uniikki ja pienimmästäkin tiedon muutoksesta se muuttuu merkittävästi, joten sitä voidaan käyttää tiedon eheyden tarkistamiseen tai salausprosesseissa. (Wagner 2022.)

**Shard** tarkoittaa tietuesta jaettua pienempää osaa. Esimerkiksi kryptovaluuttalompakon yksityisavaimen jakaminen shardeihin tarkoittaa yksityisavaimen pilkkomista useampaan osaan, jotka yhdessä muodostavat alkuperäisen yksityisavaimen. Esimerkiksi jos yksi shard varastetaan, varastetulla osalla ei ole merkitystä ilman muita shardejia. Tämä lisää turvallisuutta ja

estää yksityisavaimen täydellistä palauttamista tilanteessa, jossa yksi shard varastetaan. (Krayon Digital 2023.)

**Ticker** on yleisesti käytetty termi, joka viittaa kryptovaluutan tai pörssiyhtiön lyhyiseen tunnusmerkintään. Ticker on yleensä muutaman kirjaimen pituinen merkintä, joka helpottaa kryptovaluutan identifioimista ja erottamista muista valuutoista. Esimerkiksi Bitcoinin tunnusmerkintä on BTC, Ethereum on ETH ja Ripple on XRP. Nämä tunnusmerkinnät ovat yleisesti käytössä kryptovaluutan hintojen, markkina-arvojen ja muiden tietojen ilmoittamisessa. (Alexandria 2023.)

## 2 Kryptovaluutat ja riskit

Tämän opinnäytetyön tietoperustana ovat erilaiset Bitcoinista ja kryptovaluutoista kertovat lähteet. Kerron Bitcoinin ja kryptovaluuttojen syntymästä, niiden turvallisuudesta sekä keinoista, miten niitä pystytään säilyttämään ja käsittelemään turvallisesti.

Kerron myös yritysturvallisuuden ja riskienhallinnan perusteista sekä kryptovaluuttojen kirjanpidosta ja verotuksesta. Tietoperusta antaa suuntaa kryptovaluutoista sekä niiden turvallisuudesta. Myöhemmin opinnäytetyössäni käyn läpi puolistrukturoitujen asiantuntijahaastatteluiden vastauksia, joiden tukena on hyvä lukea läpi tietoperusta, jotta lukija ymmärtää paremmin tuloksia.

### 2.1 Bitcoin ja kryptovaluuttojen historia

Bitcoin luotiin vuonna 2008 nimettömänä pysyvän pseudonyymin Satoshi Nakamoton toimesta tarkoituksena toimia täysin vertaisverkossa toimivana käteisenä ilman kolmansien osapuolten, kuten rahoituslaitoksien, puuttumista transaktioihin (Nakamoto 2008, 1). Bitcoin edustaa ensimmäistä oikeasti vartenotettavaa ratkaisua digitaaliseksi rahaksi (Ammous 2019, 227).

Satoshi Nakamoto totesi, että hän siirtyy uusiin projekteihin ja katosi vuoden 2010 puolivälissä. Tämän jälkeen hänestä ei ole kuulunut mitään, ja Nakamoton Bitcoin-lompakon noin miljoona bitcoinia ei ole siirtynyt sen jälkeen. Tähän päivään mennessä ei ole mitään tietoa, kuka Nakamoto on tai oli, koska hän oli erittäin varovainen siitä, ettei häntä tunnisteta. Toinen Bitcoinin alkuperäisistä kehittäjistä, Hal Finney, menehtyi vuonna 2014, joten voidaan todeta, että Bitcoin on toiminut jo yli 8 vuotta ilman minkäänlaista keskushallintoa tai ylintä päättävää elintä tehden siitä todellisesti hajautetun kryptovaluutan. (Ammous 2019, 344-345.)

Ennen Bitcoinin keksimistä voitiin jakaa maksutavat kahteen luokkaan:

1. Käteismaksut, jotka ovat välittömiä ja lopullisia lähtökohtaisesti kahden henkilön välisiä suorituksia. Nämä maksut eivät vaadi osapuolten välistä luottamusta, maksusuorituksessa ei ole viivettä eikä maksujen väliin pysty mikään kolmas osapuoli tulla pysäyttämään maksua. Käteismaksujen heikkous on fyysisen läsnäolon tarve maksua varten. (Ammous 2019, 229.)
2. Välitetyt maksut, jotka vaativat kolmanteen osapuoleen luottamista ja jotka koostuvat muun muassa pankkikorteista, luottokorteista, pankkisiirroista ja rahanvälityspalveluista. Etu välitetyissä maksuissa on kahden osapuolen välinen transaktio ilman fyysisen läsnäolon tarvetta ja mahdollisuus maksun suorittamiseen ilman rahojen mukana kantamista. Välitettyjen maksujen heikkous kolmanteen osapuoleen luottamisen lisäksi ovat maksun viive ja välityskustannukset. (Ammous 2019, 229-230.)

Ennen Bitcoinin keksimistä kaikki digitaaliset maksut sisältyivät välitettyihin maksuihin. Kaikki sähköiset maksut piti kierrättää kolmansien osapuolten kautta kaksoismaksamisen ehkäisemiseksi. Kolmannen osapuolen tehtävä oli seurata tiliä ja varmistaa jokaisen rahasiirron oikeellisuutta. Digitaaliset maksut olivat siis kolmansien osapuolten tarkkailun alla, kun taas käteisvaihdot olivat suoraan kontaktiin ja fyysiseen läsnäoloon sidottuja. (Ammous 2019, 230.)

Bitcoin oli ensimmäinen ratkaisu, jota voitiin kutsua digitaalseksi käteiseksi, sen mahdollistaessa digitaaliset maksut ilman tarvetta kolmannelle osapuolelle. Bitcoin on absoluuttisen niukka ja varmennettavissa oleva digitaalinen esine. (Ammous 2019, 230-231.)

Bitcoin on myös ensimmäinen likvidi hyödyke, jolle on asetettu maksimimäärä, jota ei voi lisätä. Yleinen harhakäsite Ammousin (2019, 241) mukaan on se, että mikä tahansa hyödyke olisi rajallinen tai niukka, koska mikä tahansa hyödykkeen tuotantorajoite ei perustu sen esiintymiseen maailmassa, vaan sen tuotannon ajan ja vaivan panostukseen.

Kolmansien osapuolien käyttäminen rahan vaihdossa on heikennys turvallisuuteen ja jättää osapuolet haavoittuvaisiksi poliittisille kielloille ja seurannalle. Aikaisemmin tehdessä digitaalista siirtoa ei ollut mahdollista olla luottamatta kolmansiin osapuoliin, vaan piti hyväksyä riski siitä, että maksun siirto voitiin pysäyttää vedoten terrorismiin tai rahanpesuun. (Ammous 2019, 231.)

Bitcoinin luoja, Satoshi Nakamoton, tavoite oli luoda Bitcoinista ”puhtaasti vertaismuotoinen elektroninen käteinen”, jonka tarjontaa mikään muu osapuoli ei pystyisi muuttamaan eikä vaatisi luottamusta kolmanteen osapuoleen. Nakamoto onnistui tässä hyödyntämällä tiivistefunktiolaskentaa (engl. hashing), hajautettua vertaisverkkoa (engl. Peer-to-Peer eli P2P) ja työntodistetta (engl. Proof-of-Work eli PoW). (Ammous 2019, 232.) Käsittelen laajemmin PoW:n käsitettä luvussa 2.2.6.

Bitcoinin lohkot lisätään lohkoketjuun noin kymmenen minuutin välein. Bitcoin-verkon syntyhetkellä vuonna 2009 lohkopalkkio oli 50 bitcoinia lohkoa kohden. Noin neljän vuoden välein, tai tarkemmin aina 210 000 lohkon välein lohkopalkkio puolittuu. Ensimmäisen puolittumisen jälkeen vuonna 2012 lohkopalkkio oli 25 bitcoinia lohkoa kohden, vuonna 2016 12,5 bitcoinia ja vuonna 2020 6,25 bitcoinia. Tarjonta jatkaa nousuaan laskevaan tahtiin aina noin vuoteen 2140 asti, jolloin uusia bitcoineja ei enää lasketa liikkeelle. (Ammous 2019, 243.)

Bitcoinin maksimimäärä on siis 21 miljoonaa bitcoinia, tehden Bitcoinista deflatorisen. Tätä maksimimäärää ei pysty muuttamaan, jos ei suurin osa Bitcoin-verkosta hyväksyisi tällaista muutosta. Näillä näkymin yleinen tahtotila on se, että tällaista tai muita radikaalisia muutoksia ei tehdä Bitcoinin toimintaperiaatteeseen. (Singh 2021.)

Yhden bitcoinin voi jakaa 100 000 000 desimaaliin, tai satoshiin Bitcoinin luoja Satoshi Nakamoton pseudonyymillä, tehden siitä myytävää kaikissa mittakaavoissa, myös tulevaisuudessa sen kasvaessa arvossaan fiat-valuuttoihin verrattuna. (Ammous 2019, 243 ja 246.)

#### 2.1.1 Ethereum ja muut kryptovaluutat

Kaikkia muita kryptovaluuttoja kutsutaan altcoineiksi. Suuri osa altcoineista ovat klooneja Bitcoinin lohkoketjusta pienin muutoksin. Esimerkkejä muutoksista voivat olla kolikon tarjonta, tiivistefunktio ja lohkoaika. (Karame & Androulaki 2016, 163-164.)

Ethereum julkaistiin vuonna 2015 rakentuen Bitcoinin tavoin lohkoketjuteknologiaa käyttäväksi kryptovaluutaksi. Erona Bitcoiniin on muun muassa se, että Ethereum on ohjelmoitavissa, ja Ethereumin verkkoon voi ohjelmoida sekä julkaista hajautettuja sovelluksia. Käytännössä siis Ethereumin lohkoketjussa voi säilyttää tietoja tai määrittää mitä hajautettu sovellus tekee ilman, että kolmansia osapuolia pääsee käsiksi tietoon. (Ethereum 2022.) Tätä kirjoittaessa Ethereum on toiseksi suurin kryptovaluutta Bitcoinin jälkeen (CoinMarketCap 2023a).

Litecoinin lähdekoodi on kopio Bitcoinista kolmella muutoksella. Litecoin-verkossa lohko luodaan 2,5 minuutissa Bitcoinin 10 minuutin lohkoajan sijasta, maksimitarjonta on 84 miljoonaa litecoinia ja tiivistefunktiona toimii Scrypt Bitcoinin SHA256:n sijasta. Litecoinin lyhyempi lohkoaika mahdollistaa nopeammat transaktioiden varmennusajat mahdollistaen Litecoinin käytön paremmin esimerkiksi maksutapana kaupoissa. Eri tiivistefunktio tarkoittaa myös sitä, että samoilla ASIC-laitteilla ei voi louhia Bitcoinia ja Litecoinia. (Karame & Androulaki 2016, 164.)

Dogecoin on myös kopio Bitcoinista, jonka tarkoitus oli alun perin olla vitsi. Tämän takia Dogecoinia usein kutsutaan meemikolikoksi. (Chohan 2021, 1-2.) Dogecoin on kuitenkin täysin toimiva kryptovaluutta 1 minuutin lohkoajalla ja 100 miljardin Dogecoinin

maksimitarjonnalla. Dogecoin soveltuu myös hyvin tippausvaluutaksi verkossa, eli käyttäjät voivat antaa tippiä helposti sisällönluojille verkossa. (Karame & Androulaki 2016, 164-165.)

Muita suosittuja kryptovaluuttoja ovat muun muassa Binance Coin (BNB), joka on Binance-kryptovaluuttapörssin oma kryptovaluutta ja CoinMarketCapin (2023a) mukaan neljänneksi suurin kryptovaluutta. Tämän jälkeen CoinMarketCapin (2023a) mukaan tulevat suuruusjärjestyksessä XRP, Cardano, Polygon, Dogecoin, Solana ja Polkadot. Näiden lisäksi välissä olivat vakaavuudet Tether, USD Coin ja Binance USD, jotka ovat kaikki Yhdysvaltojen dollariin sidottuja vakaavuuttoja (CoinMarketCap 2023a). Vakaavuuttojen (engl. stablecoin) funktio on käyttää, siirtää ja vastaanottaa dollareita kryptovaluuttojen tavoin lohkoketjun avulla (Hayes 2022).

Bitcoinista on myös haarautettu (engl. fork) uusia valuuttoja, kuten Bitcoin Cash, muuttaen esimerkiksi lohkokokoa yhdestä megatavusta kahdeksaan megatavuun. Nämä haarautumiset Bitcoinista eivät ole kuitenkaan onnistuneet eduistaan huolimattaan syrjäyttämään Bitcoinin ykköspaikkaa muun muassa Bitcoinin vankan kannattajajoukon ja muuttumattomuutensa takia. (Ammous 2019, 310-313.)

Bitcoinin lähdekoodi on avoin, mutta Bitcoinin muuttamattomuus perustuu verkon konsensusääntöihin, joihin jokainen verkossa oleva solmu (engl. node) sitoutuu. Jos lähdekoodiin tulee jotain parannuksia, niin suurin osa verkon solmuista tulisi myös hyväksyä parannukset, jotta ne voidaan lisätä Bitcoinin lähdekoodiin. Jos joukko solmuja ei hyväksy muutoksia tai ottavat käyttöönsä uuden konsensusäännön, sitä kutsutaan hard forkiksi. (Ammous 2019, 304-305.)

Viimeisin esimerkki hard forkista on Ethereumin merge-tapahtuman luoma haarautuminen Ethereumista ETHPoW-valuutaksi (ticker ETHW). Osa Ethereumin käyttäjistä eivät hyväksyneet merge-tapahtumaa, eli Ethereumin työntodistemallista siirtymistä PoS-konsensusmekanismiin, vaan he haarauttivat Ethereumista oman lohkoketjunsä, joka säilyttää koko Ethereumin lohkoketjun historian, mutta merge-tapahtumasta alkaen ETHW-lohkoketju jatkaa työntodistemallia mahdollistaen sen louhimista jatkossakin näytönohjaimilla tai ASIC-laitteilla, kun taas ETH-lohkoketju jatkaa PoS-konsensusmekanismilla. (Katte 2022.) Uusi ETHW-valuutta ei kuitenkaan nostonut tuulta alleen heti merge-tapahtuman jälkeen sen fiat-arvon ollessa murtoosa Ethereumin arvosta. Kirjoitushetkellä yhden Ethereumin arvo on noin 1300 Yhdysvaltain dollaria, kun taas yhden ETHW:n arvo on vain noin 10 dollaria (CoinMarketCap 2023a).

### 2.1.2 Skaalausratkaisut ja Bitcoinin tulevaisuus

Bitcoinin nykyinen lohkokoko on rajattu yhteen megatavuun, tehden bitcoinin maksimipäiväkapasiteetiksi noin 500 000 siirtoa. Tämä raja on kuitenkin tullut vastaan, mutta se ei ole hidastanut bitcoinin arvon kasvua. Tästä voidaan Ammousin (2019, 253) mukaan päätellä, että käyttäjät pitävät bitcoinia enemmän arvon säilyttäjänä kuin vaihdannanvälineenä.

Bitcoinin siirtokulujen ollessa korkeita, bitcoin ei edes sovellu sellaisenaan nopeaan päivittäiseen maksamiseen. Jotta Bitcoin voisi edes teoriassa käsitellä yhtä paljon tapahtumia kuin esimerkiksi Visa, tulisi jokaisen lohkon olla noin 800 megatavua. Tämä tarkoittaa sitä, että vuodessa jokainen solmu lisäisi noin 42 teratavua lohkoketjuun. Tämä on nyt ja tulevaisuudessakin täysin mahdotonta saatavilla olevilla tietokoneilla. (Ammous 2019, 318.) Tätä varten bitcoinverkon päälle on kehitetty uusia skaalausratkaisuja. Yksi tunnetuimpia skaalausratkaisuja on Lightning Network, tai suomeksi Salamaverkko. (Ammous 2019, 324.)

Salamaverkko mahdollistaa maksukanavien perustamisen suoraan Bitcoin-solmujen välillä, jolloin transaktioita ei kirjata suoraan lohkoketjuun, vaan lohkoketjussa ainoastaan vahvistetaan osoitteiden saldot kanavien avaus- ja sulkemishetkellä (Ammous 2019, 325). Salamaverkon vahvuus on siinä, että maksukanavan perustaminen ja sulkeminen vaatii ainoastaan kaksi kirjattavaa tapahtumaa lohkoketjuun sallien rajattomien bitcointapahtumien suorittamisen tehokkaasti lohkoketjun ulkopuolella. Kanavien avaaminen ja sulkeminen on myös joustavaa, niitä voidaan avata ja sulkea kysynnän mukaan. Lohkoketjun ulkopuolinen tapahtuma ei kuitenkaan ole yhtä turvallinen kuin suoraan lohkoketjuun kirjattava tapahtuma. (Ammous 2019, 397-398.)

Suurin osa skaalautuvista maksuista tapahtuvat kuitenkin Ammousin (2019, 320) mukaan lohkoketjun ulkopuolella, eli pienet maksut tapahtuvat palveluiden, kuten kryptovaluuttapörssien ja -nettikasinon sisällä, lohkoketjun ulkopuolella. Tällaiset pörssipalvelut ja nettikasinot kirjaavat lohkoketjuun lähinnä ulosmeneviä ja sisään tulevia maksuja, muuten kaikki kryptovaluuttaliikenne tapahtuvat niiden sisäisissä tietokannoissaan (Ammous 2019, 386).

Huomion arvoista skaalausratkaisussa on riski Bitcoinin tuoman verkon sensuroimattomuuden menettämiselle. Bitcoin on ensimmäinen aidosti luotettava teknologia arvon siirtämiselle digitaalisesti ilman välikäsiä. Vaikka Bitcoin-verkko itsessään pystyy käsittelemään ainoastaan muutamia satoja tuhansia tapahtumia päivässä, niin kaikki välikädet ja kolmannet osapuolet, jotka kasvattavat bitcointapahtumien maksimimäärää, voivat teoriassa sensuroida ihmisten tekemiä bitcoinsiirtoja. (Ammous 2019, 401-402.)

Toinen riski on verkon hajautuksen menetys. Jos suurin osa ihmisistä luottaisivat jatkossa kolmansiin osapuoliin, jotka tarjoavat skaalausratkaisua, niin Bitcoin ei olisi enää vertaisverkko, vaan yritykset tai muut tahot voisivat helpommin vaikuttaa Bitcoinin konsensussääntöihin pääverkossa. (Ammous 2019, 402.)

## 2.2 Kryptovaluuttojen ja lohkoketjujen turvallisuus

Kryptovaluuttojen turvallisuus on helppo varmentaa avointen lähdekoodien avulla. Esimerkiksi Bitcoin itsessään on avoin protokolla, jonka lähdekoodia kuka tahansa pystyy käymään itse läpi varmistaen, ettei lähdekoodissa ole minkäänlaisia aukkoja tai takaportteja. Keskitettyjen

palveluiden, kuten kryptovaluuttapörssien ja lainapalveluiden, käyttö edellyttää luottamusta kolmannen osapuolen palvelua kohtaan.

Seuraavissa alaluvuissa käyn läpi kryptovaluuttojen salausta, lompakoiden palauttamista muistitekniesten sanojen avulla, avainten jakamiskeinoja, transaktioiden turvallisuutta, yksityisyyttä, louhimisprotokollia, 51 % -hyökkäystä, keskitettyjä kryptovaluuttapalveluja sekä kryptovaluuttalompakoita.

### 2.2.1 Salaus

Liittyessään bitcoinverkkoon, käyttäjä luo itselleen julkisen osoitteen ja yksityisen avaimen. Ihmiset voivat lähettää bitcoineja muille, kun vastaanottajan julkinen osoite on tiedossa. Ainoastaan silloin, kun käyttäjällä on Bitcoin-lompakon yksityisavain tiedossa, käyttäjä voi käyttää ja lähettää lompakon varoja muille. Sekä julkinen osoite että yksityisavain voidaan esittää QR-koodina. (Ammous 2019, 295-296.)

Bitcoin-osoite muodostuu 26-35 alfanumeerisesta merkistä ja ensimmäinen numero tai ensimmäiset merkit ovat 1, 3 tai bc1. Jokainen Bitcoin-osoite muodostetaan ECDSA-avaimesta (Elliptic Curve Digital Signature Algorithm), josta Bitcoin-lompakon omistaja tietää vastaavan yksityisen avaimen. (Karame & Androulaki 2016, 33-34.) Käytännössä osoite pohjautuu Base58-salauksen tiivisteseen julkisesta avaimesta. 1-alkuiset osoitteet ovat alkuperäisiä (engl. legacy) osoitteita, 3-alkuiset osoitteet ovat ”Nested SegWit” tai niin sanottuja Multisig-osoitteita (Karame & Androulaki 2016, 38) ja bc1-alkuiset osoitteet ovat natiiveja SegWit-osoitteita (Min 2021).

### 2.2.2 BIP-39

BIP-39 (2013) parannusehdotus käsittelee muistitekniesten sanojen (engl. mnemonic words) käyttöönottoa Bitcoinille. Kyseinen parannus ehdotettiin sen takia, että lompakon palauttaminen olisi helpompaa sanoilla kuin pitkällä heksadesimaalisilla palautusavaimilla. Muistitekniesten sanat ovat helpompia myös kirjoittaa ylös, muistaa tai luetella ääneen.

BIP-39 (2013) sanaluettelolla on seuraavat ominaisuudet:

- Älykäs sanavalinta: Sanan neljä ensimmäistä kirjainta riittävät sanan tunnistamiseen. Lompakkosovellus voi esimerkiksi täydentää automaattisesti sanan, kun neljä ensimmäistä kirjainta on kirjoitettu, koska kahta samanlaista sanaa ei löydy sanaluettelosta, joissa olisi samat neljä ensimmäistä kirjainta.
- Samanlaisia sanoja vältetään: Sanaparit, kuten hidas ja hitaasti, tai mies ja miehiä, kasvattavat virheen mahdollisuutta ja ovat vaikeampia muistaa.

- Lajitellut sanalistat: Sanaluettelo on lajiteltu, joka mahdollistaa nopeamman ja tehokkaamman sanojen haun luettelosta.

Sanalistoja löytyy englannin lisäksi japaniksi, koreaksi, espanjaksi, kiinaksi, ranskaksi, italiaksi, tšekiksi ja portugaliksi, mutta useimmat lompakot tukevat vain englanninkielistä sanalista, joten ei ole suositeltua käyttää normaalisti muunkielistä listaa. Sanalista voi myös sisältää alkuperäisiä merkkejä, mutta ne täytyy silti koodata UTF-8-koodauksella. (BIP-39 2013.)

BIP-39 (2013) sanaluettelo sisältää 2048 sanaa. Todennäköisyys keksiä esimerkiksi sama 24:n sanan avain kuin toisella on siis  $1:2048^{24}$ , eli hyvin epätodennäköinen ellei jopa mahdoton. Yhtäkään tällaista tapausta ei ole tullut vastaan, että joku olisi keksinyt toisen olemassa olevan muistitekniikan palautusavaimen.

Muistitekniiset sanat ovat jääneet yleiseksi tavaksi palauttaa kryptovaluuttalompakko myös suurimmalle osalle muita kryptovaluuttoja, ei pelkästään Bitcoin-lompakoille. Tämä tekee BIP-39:stä avoimen standardin, jota suosituimmat kryptovaluuttalompakot käyttävät. (Behnke 2022a.)

### 2.2.3 Avainten jakaminen

Moniallekirjoituksellinen (engl. multisignature), eli Multisig-transaktio vaatii useamman kuin yhden allekirjoituksen, jotta transaktio toteutuisi (Karame & Androulaki 2016, 40). Multisig-osoitteet ovat liitettyinä useampaan kuin yhteen ECDSA-yksityisavaimen. Pääasiallinen tarkoituksena moniallekirjoituksille on korkeampi kryptovaluuttojen varastamisen vaikeus. Yksityisavaimet voidaan esimerkiksi säilyttää hajautetusti usealla erillisellä tietokoneella tai usean henkilön hallussa. Moniallekirjoituksia voi myös käyttää silloin, kun halutaan jakaa yksi lompakko useamman henkilön kesken ja halutaan vaatia enemmistöltä allekirjoituksen, jotta transaktio toteutuisi. (Karame & Androulaki 2016, 149-150.)

Multisig-lompakon voi luoda ainakin Electrum-lompakko-ohjelmassa ja transaktioita pystyy myös Trezor-laitelompakossa allekirjoittamaan. Electrum tukee myös Ledger- ja Digital Bitbox-laitelompakkoita moniallekirjoituksissa, mutta Saleem Rashidin (2018) mukaan ainoastaan Trezor toimii moitteettomasti tässä.

Multisig-lompakkoa uudempi ratkaisu ovat MPC-lompakot. MPC on lyhenne sanoista Multi-Party Computation tai suomeksi monen osapuolen laskenta. Rob Behnke (2022b) kuvailee MPC-lompakkoita uudemaksi tavaksi turvata kryptovaluuttavarat tasapainottaen turvallisuuden ja tehokkuuden. MPC-lompakko on kryptovaluuttalompakko, joka vaatii useamman tahon valtuuttamaan transaktioita, eli sama periaate kuin Multisig-lompakoissa, sillä eroavaisuudessa, että jokainen allekirjoitusosapuoli käyttää myös hajautettua laskentaprotokollaa. MPC-lompakot eivät myöskään ole sidottu yhteen yksityiseen avaimen, vaan yksityisen avaimen

osuudet jaetaan allekirjoitusosapuolten kesken. MPC-lompakot soveltuvat myös hyvin jokapäiväiseen kryptovaluuttojen käyttöön paremmalla tehokkuudella, koska yksityisen avaimen osuuden säilyttäminen verkossa ei vaaranna lompakkoa, vaikka yksi osuus päätyisi väärin käsiin.

Multisig- ja MPC-lompakot ovat hyvin samankaltaisia periaatteeltaan, molemmat käyttävät  $m$ -of- $n$ -allekirjoitusjärjestelmää, eli tarvitaan tietty määrä allekirjoittajia, että transaktio voidaan hyväksyä. MPC-lompakot voivat toimia useimpien lohkoketjujen kanssa, jotka toteuttavat EdDSA- tai ECDSA-allekirjoitusalgoritmia, kun taas Multisig-lompakot eivät ole yhteensopivia kaikkien lohkoketjujen kanssa. MPC-lompakoiden allekirjoitus tapahtuu myös lohkoketjun ulkopuolella, parantaen allekirjoitusosapuolten yksityisyyttä. Multisig-transaktioissa allekirjoitukset ovat saatavilla ketjussa, edesauttaen haitallisia osapuolia allekirjoitusosapuolten jäljittämässä. MPC-transaktiot tarvitsevat myös lohkoketjussa vain yhden allekirjoituksen tehden transaktiokuluista yhtä suuret kuin normaaleissa kryptovaluuttatransaktioissa, kun taas Multisig-transaktiot vaativat useamman allekirjoituksen, tehden tapahtumien siirtokuluista isompia. (Behnke 2022b.)

Suurin etu MPC-lompakoissa yritysten näkökulmasta on helpompi hallinnollisuus kuin Multisig-lompakoissa. Multisig-lompakoissa useiden avainten määrittely on pysyvää. Jos halutaan muuttaa hyväksymiskynnys Multisig-lompakossa esimerkiksi viidestä neljään allekirjoitusosapuoleen, niin joudutaan luomaan uusi Multisig-lompakko ja siirtämään varat vanhasta lompakosta siihen. MPC-lompakot mahdollistavat joustavamman hyväksymiskäytännön, eli lompakon osoite ei muutu eikä varoja tarvitse siirtää mihinkään, jos halutaan muuttaa avainosuuksia. (Behnke 2022b.)

Fireblocks ja ZenGo ovat suosittuja MPC-lompakoiden tarjoajia. Fireblocks (2023) tarjoaa MPC-lompakkoa palveluna yrityksille. Fireblocks tarjoaa yrityksille muun muassa REST API:a automaattisia talletuksia ja nostoja varten, 30 eri julkista ja yksityistä lohkoketjuprotokollaa ja yli 1100 tokenia sekä SaaS-, hybridi- ja On-prem-ylläpitoratkaisuja. ZenGo (2023) tarjoaa helpommin lähestyttävissä olevaa sovellusta ilmaiseksi myös yksityiskäyttäjille sisäänrakennetulla MPC-teknologialla. ZenGo mainostaa olevansa ensimmäinen MPC-kryptovaluuttalompakko, jonka avulla käyttäjän ei tarvitse käsitellä perinteisiä haavoittuvia yksityisavaimia.

Ethereum-puolella suosittu avoimen lähdekoodin Multisig-lompakko on Gnosis Safe (2023). Ominaisuudet ovat pitkälti samanlaiset kuin yllä olevilla ratkaisuilla, sillä erolla, että Gnosis Safessa voi implementoida Multisig-allekirjoitukset myös DeFi-puolelle ja NFT:iden säilytystä varten.

Yksi keino yksityisavaimen varmuuskopioimiseksi useamman tahon kesken on menetelmä nimeltään Shamir's secret-sharing (lyh. SSS), joka on nimetty tunnetun kryptografian Adi Shamirin mukaan, jonka salausmenetelmiään jakojen luomiseksi käytetään hyödyksi. SSS jakaa

yksityisavaimen useaan yksilölliseen osaan, jotka voidaan jakaa eri käyttäjille. Avainta jaettaessa määritellään, kuinka monta osuutta luodaan, sekä kuinka monta näistä osuuksista tarvitaan alkuperäisen salausavaimen uudelleenluomiseksi. Alkuperäistä salausavainta ei pysty luomaan uudelleen, jos vaadittavaa minimimäärää SSS-osia ei ole hallussa. Tällöin ei ole pääsyä myöskään kryptovaluuttalompakkoon, vaikka minimimäärän alittava määrä SSS-osia vuotaisi pahansuovalle taholle. (Rusnak ym. 2017.)

Bitcoinin tapaisissa hajautetuissa maksujärjestelmissä kryptovaluuttalompakoiden varmuuskopioiden eheys ja saatavuus on erityisen tärkeää, koska kryptovaluuttavaroja ei pystytä palauttamaan, jos pääsy lompakkoon estyy tai pahansuopa taho pääsee niihin käsiksi. Normaalisti useampi varmuuskopio useassa eri paikassa olisi riittävä toimenpide yksityisavaimen turvallisuudelle säilytykselle, mutta koska likvideihin varoihin pääsisi käsiksi suoraan varmuuskopioidusta avaimesta, voi pääsy yhteen varmuuskopioon olla riittävä askel kaikkien sen yksityisavaimen sisältävän kryptovaluuttalompakon varojen pysyvään katoamiseen. SatoshiLabs on ehdottanut SLIP-39-ehdotuksessaan, että heidän SSS-metodinsa korvaisi avoimena standardina BIP-39:n, eli muistitekniset sanat. (Rusnak ym. 2017.)

Christopher Allenin ja Mark Friedenbachin (2019) mukaan sosiaalisen avaimen palautuksen toteutus tulisi vaatia useamman henkilön hyväksyntä vähentääkseen avainten väärinkäytön mahdollisuutta sekä edellyttää pienintä mahdollista kynnystä estääkseen varojen menetys tuhoutuneiden tai kadonneiden osien vuoksi. Ei ole kuitenkaan toivottavaa, että avaimen osia annetaan liian monelle taholle, koska SSS-osat joudutaan luomaan kaikille uusiksi, jos yhden tahon pääsy täytyy estää. On myös huomioitava sosiaalinen luotettavuus avaimia jaettaessa: ystävät, perheenjäsenet ja yritysten avainhenkilöt ovat eri asemassa, kun punnitaan ihmisten luotettavuutta avainten säilyttäjinä.

Allen ja Friedenbach (2019) tuovatkin esille esimerkin kolmisuuntaisesta lineaarisesta avainjako- ja jakamalla X-, Y- ja Z-osuuksia. X-osuudet annetaan perheenjäsenille, Y-osuudet annetaan ystäville ja Z-osuudet jaetaan vielä edelleen niin, että Z-osuuksia jaetaan jokaiselle perheenjäsenelle, ystävälle sekä luotettavalle yhtiökumppanille. Näin jokainen perheenjäsenellä on yksi X- ja Z-osuus, jokaisella ystävällä on yksi Y- ja Z-osuus ja yhtiökumppanit tietävät vain yhden Z-osuuden. Koska alkuperäinen avain on jaettu X+Y+Z-ryhmiin, tulisi kaikki rekonstruoida, joka vaatii ainakin yhden perheenjäsenen, yhden ystävän sekä yhteensä kolme tahoa mistä tahansa ryhmästä.

Pääavaimen voisi myös Rusnakin ym. (2017) mukaan salata tunnuslauseella lisäsuojauksen mahdollistamiseksi. Rusnakin ym. (2017) ehdotuksessa ei kuitenkaan tueta BIP-39:n tavoin lokalisaatiota, vaan heidän ehdotuksensa koskee vain englanninkielisiä sanoja, mutta muuten ehdotuksen sanaluettelo määrittyy melkein samoilla kriteereillä kuin BIP-39:n sanaluettelo. Sanaluettelo sisältää kuitenkin eri sanoja kuin BIP-39-sanaluettelo.

SSS on ainakin Trezor (2022) Model T -laitelompakoissa vaihtoehtona varmuuskopiota luodessa. Trezorissa (2022) voi luoda 16 SSS-osuutta, joista jokaisessa osuudessa on 20:stä 33:een muistitekniikasta sanaa ja vaadittavien osuuksien minimimäärä voidaan vapaasti valita. Trezor (2022) käyttää myös erillistä sanaluetteloa kuin tavallisissa BIP-39 varmuuskopioissa. Trezorin laitelompakko tukee myös vakiona Multisigin käyttöä, joten jokaisella yrityksen avainhenkilöllä voisi olla oma Trezor Model T -laitelompakko, jota vaaditaan Multisig-transaktioiden allekirjoittamiseen ja joiden yhteisestä yksityisavaimesta on tehty SSS-varmuuskopio-osuudet (SatoshiLabs 2019). On hyvä kuitenkin huomioida, että Trezor käyttää SSS-osuuksissa omaa SLIP-39-sanalista BIP-39-sanalistan sijasta, eikä SatoshiLabsin SLIP-39 ehdotus ole standardi. Tällä on merkitystä varsinkin, jos haluaa palauttaa toiseen laite- tai ohjelmistolompakkoon Trezorilla luodun SSS-varmuuskopion. (Blockplate 2022.)

Yksi keino turvata kryptovaluuttavarojen turvallinen saavutettavuus on käyttää Multisig-varmuuskopiota varten ulkoista palvelua. Yksi suosittu palvelu on Casa, varsinkin yrityksiä varten. Casa (2023) mainostaa olevansa ”maailman ensimmäinen henkilökohtainen avainmanageri”, joka tekee yrityksen Bitcoineista resilienssiä tarjoamalla useampaa avainta useaan paikkaan ylimääräiseksi suojaksi katoamista vastaan. Multisig-avainosuuksia voidaan säilyttää esimerkiksi puhelimesta, laitelompakossa ja Casa-palvelussa. Jos avainosuuksia katoaa tai varastetaan, niin Casan sovellus ohjaa käyttäjää luomaan uuden osuuden vanhan tilalle. Turvallisuutta voi parantaa entisestään säilyttämällä useammassa eri paikassa ja useammalla eri laitteella avaimia. Casan palvelu Multisig-ominaisuudella on maksullinen ja räätälöitävissä yrityksen tarpeeseen.

Toinen samankaltaista palvelua kuin Casaa tarjoaa Unchained Capital (2023). Unchainedin Vault-palvelussa käyttäjä voi luoda useampia holveja, joissa on Multisig-osuus ja muut osuudet ovat käyttäjällä. Tavanomaisten allekirjoitusten lisäksi, joissa ei tarvita Unchainedia allekirjoitusosapuolena, voidaan myös luoda holveja, joissa palvelu vahvistaa henkilöllisyyden transaktioita varten.

#### 2.2.4 Transaktiot

Bitcoin-verkossa transaktioita on noin yksi sekunnissa tehden yhdestä lohkokosta melkein 400 kilotavun kokoisen. Maksimi lohkokoko Bitcoin-verkossa on 1 megatavu, tarkoittaen maksimiksi transaktioiden määräksi alle 7 transaktiota sekunnissa. (Karame & Androulaki 2016, 53.) Bitcoinin skaalausratkaisuilla (luku 2.1.2) voidaan kasvattaa transaktioiden määrää, tai sitten vaihtoehtona on käyttää nopeisiin maksuihin toista kryptovaluuttaa.

Käytännössä transaktio Bitcoin-verkossa toteutuu seuraavasti: käyttäjä valitsee esimerkiksi lompakkosovelluksessaan määrän bitcoineja, jotka halutaan siirtää toiseen lompakkoon. Transaktioon liitetään tiiviste edellisestä transaktiosta, joista käytettävissä olevat bitcoinit ovat siirretty maksajan Bitcoin-osoitteeseen. Tämä tapahtuu yleensä automaattisesti

lompakkosovelluksessa taustalla. Vastaanottajan julkinen lompakkoavain (eli paremmin tunnettuna julkinen Bitcoin-osoite) liitetään transaktion vastaanottajaksi. Tämän jälkeen transaktion sisään- ja ulostulo (eli mistä varat ovat tulleet ja mihin ovat nyt menossa) allekirjoitetaan maksajan yksityisellä avaimella, myös yleensä lompakkosovelluksessa taustalla. Viimeiseksi allekirjoitettu transaktio julkaistaan vertaisverkossa. (Karamé & Andrólaki 2016, 59.)

Kun vastaanottaja vastaanottaa transaktion, hän tarkistaa allekirjoituksen ja transaktion oikeellisuuden. Jos transaktio on oikea, vastaanottaja joutuu vielä odottamaan Bitcoin-verkon varmistusta transaktion oikeellisuudesta, ennen kuin vastaanottaja pystyy käyttämään vastaanotettuja varoja. Bitcoin-louhijat louhivat lohkot, joissa transaktiot ovat varmistettu, eli louhijat lisäävät uusiin lohkoihin varmistetut transaktiot. Transaktio on varmistettu verkossa ja on käytettävissä silloin, kun transaktio sisältyy kuuteen peräkkäiseen lohkoketjussa. (Karamé & Andrólaki 2016, 59-60.)

Käyttäjät joutuvat odottamaan joskus jopa 100 minuuttia, että transaktio on saanut verkosta kuusi varmennusta. Tämän takia nopeissa transaktioissa, kuten kaupoissa tai automaateissa, pitäisi edellyttää transaktiolta 0 varmistusta, joka on turvatonta (Karamé & Andrólaki 2016, 69), tai aikaisempaa mainittuja skaalausratkaisuja.

#### 2.2.5 Yksityisyys

Bitcoin-lompakot osoitteineen ovat pseudonyymisiä. Jokaisen Bitcoin-lompakon transaktiohistorian pystyy selvittämään lohkoketjussa pelkän Bitcoin-osoitteen avulla. Toisin sanoen, jos yhden Bitcoin-lompakon omistajan saa selville, saa myös selville kaikki kyseisen tahon transaktiot kyseisessä lompakossa. Jokainen käyttäjä pystyy kuitenkin luomaan rajattomasti Bitcoin-lompakoita, vaikka yhden jokaista transaktiota kohden, jolloin yksityisyys hieman paranee. (Karamé & Andrólaki 2016, 85.)

Yksityisyyttä parantavia kolmannen osapuolen palveluja on kuitenkin olemassa, kuten esimerkiksi erilaiset mikserit. Nämä ovat tunnettuja muun muassa rikollisten joukoissa, koska mikserit voivat toimiessaan taata täyden anonymiteetin transaktioille. Käytännössä tätä kutsutaan rahanpesuksi, kun yritetään piilottaa rikollisesti ansaittujen varojen alkuperää. (Nelson 2022.)

Tunnettu Ethereum-mikseripalvelu Tornado Cash (Nelson 2022) sai elokuussa 2022 sanktiot Yhdysvaltojen valtionvarainministeriöltä lamauttaen kyseisen palvelun toiminnan. Elliptic Connectin (2022) mukaan yhteensä yli 7 miljardia Yhdysvaltain dollaria oli virrannut Tornado Cashin läpi sen olemassaolon aikana, joista 1,54 miljardia dollaria liittyi varmuudella rikolliseen toimintaan, kuten varkauksiin, hakkerointeihin ja huijauksiin.

Jason Nelsonin (2022) mukaan mikserille on kuitenkin ihan laillisiakin käyttötarkoituksia: samanlailla kun esimerkiksi työnantajalle ei kuulu kaikki yksityiset pankkisiirrot ja luottokorttiostokset, niin käyttäjät haluavat todennäköisesti myös pitää salassa heidän kryptovaluutatransaktionsa. Toinen laillinen käyttötarkoitus on myös lahjoittaa nimettömästi varoja yleishyödylliseen tarkoitukseen. Jopa Ethereumin luoja, Vitalik Buterin (2022), myönsi käyttäneensä Tornado Cashia lahjoittaakseen varoja hyväntekeväisyyteen.

Tornado Cash ja muutkin mikserit toimivat niin, että käyttäjä yhdistää lompakkosovelluksensa, kuten esimerkiksi Metamaskin, mikserialustaan, valitsee verkon (Tornado Cashissa verkkovaihtoehdot olivat Ethereum, Binance Smart Chain, Polygon ja Ethereum Goerli -testiverkko) sekä haluaako tallettaa vai kotiuttaa varoja. Talletusvalinnan jälkeen tallettajalle luodaan varmenne, jota tallettaja tarvitsee nostaakseen myöhemmin varoja palvelusta. Siirto varmistetaan tämän jälkeen lompakkosovelluksessa. Nostaessaan varoja palvelusta käyttäjä syöttää saamansa varmenteen ja vastaanotto-osoitteen. (Nelson 2022.)

CoinJoin on protokolla, jonka tavoite on myös sekoittaa varoja ilman kolmatta osapuolta transaktiossa, jossa on useampi lähettäjä ja vastaanottaja. Tässä tapauksessa edellytetään kuitenkin sitä, että kaikki lähettäjät ja vastaanottajat sopivat keskenään transaktiosta. Varojen vastaanottajien määrä täytyy myös olla sama kuin lähettäjien määrä, jolloin jokainen vastaanottaja saa yhtä suuren osuuden varoja, kuin mitä jokainen lähettäjäkin on lähettänyt. Koko transaktio epäonnistuu, jos yksikin lähettäjä ei allekirjoita transaktiota. Huomioitavaa on myös se, että CoinJoin-transaktioilla on myös huomattavasti korkeammat siirtokulut useamman varmistuksen takia. (Karame & Androulaki 2016, 99-100.)

Vastaanottajan olisi myös hyvä tiedostaa mistä vastaanottaa kryptovaluuttavaroja. Rikollisessa toiminnasta saatuja kryptovaluuttoja voidaan seurata lohkoketjussa myös vastaanottajalle asti, jolloin vastaanottajan henkilöllisyyden paljastuessa voi vastaanottajallakin mahdollisesti tulla seuraamuksia, kuten jopa varojen menettäminen. Varsinkin kolmannen osapuolen säilytyspalveluissa tällaiset varat eivät välttämättä ole turvassa. (Karame & Androulaki 2016, 93.)

#### 2.2.6 PoW ja PoS

PoW, eli englannin kielellä Proof-of-Work, tarkoittaa suomeksi työntodistetta. Varmennus ja työntodiste ovat Bitcoinin tärkeimpiä ominaisuuksia, jotka poistavat luottamuksen tarpeen kokonaan. Työntodistejärjestelmä tarkoittaa sitä, että bitcoinverkon solmut kilpailevat käyttäen prosessointivoimaa siitä, kuka päivittää ensimmäisenä lohkoketjuun uuden transaktion joka kymmenes minuutti. Käytännössä solmu kuluttaa prosessointivoimaa ratkaistakseen vaikeita matemaattisia ongelmia, joita on kuitenkin helppo varmentaa. Bitcoin-verkon turvallisuus perustuu siihen, että näihin matemaattisiin ratkaisuihin kuluu suuri määrä energiaa, joka menisi hukkaan, jos lohkon yritettäisiin sisällyttää virheellisiä siirtoja. Kun solmu on

ratkaissut työntodisteen oikein ja on ilmoittanut siirrot lohkoketjuun, muut solmut verkossa äänestävät sen oikeellisuudesta. Kun tarpeeksi moni on äänestänyt lohkon hyväksynnän puolesta, solmut jatkavat lohkoketjua lisäämällä siirtoja uuteen lohkoon, joka on liitettyä edelliseen, ja ratkaisevat taas siihen uuden työntodisteen. (Ammous 2019, 233-234.)

Bitcoinin louhijat sijoittavat sähköä ja prosessointitehoa, joka suojaa verkkoa, koska heille maksetaan palkkio siitä ja Bitcoinin käyttäjät maksavat siirtomaksuja sekä ostavat bitcoineja louhijoilta, joka taas tällä tavalla rahoittaa louhijoiden toiminnan (Ammous 2019, 240).

Bitcoinin alkuaikoina Bitcoinia pystyi louhimaan kotona jopa kannettavalla tietokoneella, mutta vaikeusasteen noustessa tämä ei ole enää mahdollista. Nykyään Bitcoinia louhitaan siihen tarkoitukseen kehitetyillä ASIC-louhintalaitteilla (engl. Application Specific Integrated Circuits), jotka eivät kuluta sähköä mihinkään muuhun kuin nimenomaan Bitcoinin louhintaan. (Ammous 2019, 299.)

Vastaavasti Proof-of-Stake (lyh. PoS) tarkoittaa uusien kolikoiden louhimista ”steikkaamalla” (engl. stake), eli panostamalla, olemassa olevia varoja lohkoketjuun. Käytännössä ”steikkaajat”, tai validaattorit, varmentavat uusia lohkoja sillä perusteella, kuinka monta kolikkoa steikkaajalla on panostettuna. Erona PoW-konsensukseen, jossa tarvitaan suuret määrät prosessointitehoa lohkojen varmistamiseksi, steikkaajat saavat tuottoa panostamilleen kolikoilleen ilman prosessointitehoa pelkästään sitomalla lohkoketjuun kryptovaluutta. (Frankenfield 2022.)

Validaattorit, eli steikkaajat jotka varmentavat lohkotietoja, valitaan verkossa satunnaisesti, eli tuotto ei perustu louhijan laskentatehoon. Steikkaajan tulisi panostaa esimerkiksi Ethereum-verkossa vähintään 32 ethereumia päästääkseen validaattoriksi. Nykyisillä fiat-kursseilla 32 ethereumia on kuitenkin arvokasta, joten pienemmällä summalla pystyy myös sijoittamaan varoja erilaisiin pooleihin, joista saa poolin omia ERC-20-tokeneita vakuudeksi sijoitukselleen. (Frankenfield 2022.)

Proof-of-Stakessa lohkojen varmentajia kutsutaan validaattoreiksi. Validattori tarkistaa transaktioita, varmistaa lohkoketjun toiminnan, ylläpitää lohkoketjua ja äänestää tuloksista. Proof-of-Workissa lohkojen varmentajia kutsutaan louhijoiksi. Louhija ratkaisee transaktion tiivisteen varmentaakseen transaktioita. Louhija palkitaan uusilla kolikoilla onnistuessaan ratkaisemaan seuraavan lohkon tiivisteen ensimmäisenä. (Frankenfield 2022.)

PoS-mekanismi on suunniteltu vähentämään ympäristöhaittoja vähentämällä tarvittavaa prosessointitehon edellyttämää energiankulutusta. Esimerkiksi Bitcoinilla on kuitenkin PoW-mekanismi edelleen käytössä, joten muiden kryptovaluuttojen, kuten Ethereumin, siirtymisellä PoS-mekanismiin ei ole vaikutusta Bitcoinin energiankulutukseen. PoS-kryptovaluutoilla on kuitenkin suurempi riski joutua 51 % -hyökkäyksen kohteeksi, koska verkon turvallisuus ei ole taattu hajautetulla laskentateholla, vaan sijoitettujen varojen määrällä. (Frankenfield 2022.)

PoW:n ja PoS:n lisäksi on muitakin vähemmän tunnettuja konsensusmekanismeja. Yksi on PoS-pace, eli Proof-of-Space, toinen PoT, eli Proof-of-Time, sekä näiden yhdistelmä PoST, eli Proof of Space and Time, jota esimerkiksi Chia-lohkoketjuverkko käyttää. Lyhyesti PoST-konsensusmekanismeissa louhijalla on vapaata levytilaa järjestelmässään ja aikaa tarjota tilaa verkon validoimiseksi. PoST on uusi konsensusmekanismi, joka käyttää vähemmän energiaa ja on nopeampi kuin PoW-mekanismi. PoC, eli Proof-of-Coverage, on Helium-verkon käytössä oleva konsensusmekanismi, joka perustuu siihen, että louhijat tarjoavat langattoman maantieteellisen peiton verkolle. Helium-verkon louhijat käyttävät Hotspot-laitteita, jotka ilmoittavat tarikan sijaintinsa verkolle, ja louhijat saavat palkkion, jonka suuruus riippuu maantieteellisestä sijainnista ja verkon peitosta. (Abaday 2021.)

### 2.2.7 51 % -hyökkäys

Työntodisteen takia lohkon kirjoittamisen kustannukset ovat erittäin korkeat. Jos joku yrittäisi luoda virheellisiä siirtotapahtumia lohkoketjun lohkoihin, hän todennäköisesti tuhlaisi vain omaa prosessointitehoa ja sähköä saamatta lohkopalkkiota. Tämän takia Bitcoin ja bitcoinverkon työntodistejärjestelmä on sähkönkulutuksestaan huolimatta turvallinen. Bitcoinin lohkoketju on tähän mennessä ollut korruptoimaton ja historiasta ei löydy yhtäkään onnistunutta kaksinkertaisen kulutuksen hyökkäyksen aiheuttamaa vahvistettua tapahtumaa. (Ammous 2019, 298.)

Jotta hyökkääjä voisi lisätä omia vilpillisiä tapahtumia lohkoketjuun, hänellä pitäisi olla hallussaan suurin osa verkon laskentatehosta petoksen toteuttamiseksi ja vahvistamiseksi. Tätä hyökkäystä kutsutaan 51 % -hyökkäykseksi. Bitcoin-verkossa tällainen hyökkäys olisi voinut olla mahdollinen Bitcoinin alkuaikoina, jolloin verkon laskentateho oli hyvin pieni. Maailmanlaajuisen hajautettu louhintaverkko ja louhinnasta saavutettava arvokas louhintapalkkio suojelee Bitcoin-verkkoa 51 % -hyökkäystä vastaan, mutta muiden pienempien kryptovaluuttojen verkot voivat olla vähemmän hajautettuja mahdollistaen kyseisen hyökkäyksen. (Ammous 2019, 298-299.)

Bitcoinia ja Bitcoin-verkkoa on yritetty vuosia murtaa erilaisin tavoin siihen kuitenkaan onnistumatta. Bitcoin toimii Ammousin (2019, 302) mukaan kuitenkin vieläkin luotettavasti ja turvallisesti, eikä näin ollen ole syytä keskittyä syvällisemmin Bitcoinin turvallisuuteen, vaan voidaan todeta, että Bitcoin on todistetusti turvallisoin olemassa oleva kryptovaluutta. Muissa pienempien kryptovaluuttojen verkoissa saattaa kuitenkin olla todellinen uhka esimerkiksi 51 % -hyökkäykselle.

### 2.2.8 Keskitetyt kryptovaluuttapalvelut

Kryptovaluuttapörssit ja -välityssivustot mahdollistavat kryptovaluuttojen oston fiat-valuutalla, kuten euroilla, ja päinvastoin myymisen fiat-valuutaksi. Käytännössä käyttäjä tallettaa

sivustolle rahaa esimerkiksi SEPA-pankkisiirrolla, luotto- tai debit-kortilla, jonka jälkeen käyttäjä voi ostaa haluamaansa kryptovaluuttaa palvelussa olevalla talletuksellaan. Pörsseissä on yleensä enemmän ominaisuuksia kuin yksinkertaisemmissä välityssivustoissa. Pörsseissä voi muun muassa tehdä edistyksellisimpiä osto- ja myyntitarjouksia tai jopa suorittaa futuuri-kauppoja kryptovaluutoilla. (Karamé & Andrólaki 2016, 146.)

Välittäjät, niin kuin nimestä voikin päätellä, välittävät asiakkailleen kryptovaluuttoja, jolloin myös he yleensä ottavat enemmän transaktiomaksuja kaupoista. Välityssivustot tarjoavat myös yleensä lompakkopalvelun, eli kryptovaluutat voidaan jättää palveluun säilöön oston jälkeen. Yleensä tällaiset välityspalvelut ovat helpompia keinoja aloittelijoille aloittaa kryptovaluuttoihin tutustumisen, kuin monimutkaisemmat pörssisivustot. (Bitcoinkeskus.com 2022.)

Pisimpään Suomessa toiminut kryptovaluuttojen ostoa ja myyntiä tarjoava palvelu on Coinmotion. Prasos Oy (nyk. Coinmotion Oy) perustettiin keväällä 2012 Jyväskylässä pienen kaveriporukan toimesta tarkoituksenaan luoda suomenkielisen foorumin ja uutissivuston Bitcoinin liittyen. Toiminta alkoi Bittiraha.fi-alustan julkistamisella, joka on vielä tänäkin päivänä merkittävin suomalainen Bitcoin-uutissivusto. (Brade 2020.)

Prasos Oy osti Coinmotion-alustan liiketoimintakaupassa vuonna 2016. Tätä ennen Prasosin Bitcoinien osto- ja myyntipalvelut olivat toimineet Bittiraha.fi-palvelussa. Coinmotion mahdollisti turvallisen alustan asiakkaiden Bitcoineille ja se oli teknisesti kehittyneempi kuin Bittiraha.fi-alusta. Coinmotion-alustan kysyntä kasvoi nopeasti ja siitä tuli Prasos Oy -konsernin isoin palvelu. (Brade 2020.)

Prasos Oy sai Finanssivalvonnasta heinäkuussa 2019 maksulaitoksen toimiluvan ja samana vuonna Prasos Oy rekisteröitiin virtuaalivaluutan tarjoajaksi (Brade 2020). Finanssivalvonta (2019) on katsonut toimilupaa myöntäessään, että Prasos Oy:llä on ollut riittävästi resursseja rahanpesun ja terrorismin rahoittamisen torjuntaan.

Finanssivalvonta (2019) myönsi samaan aikaan Prasos Oy:n lisäksi myös virtuaalivaluutan tarjoajille Prasos Cash Management Oy:lle, LocalBitcoins Oy:lle, NorthCrypto Oy:lle sekä Tesseract Group Oy:lle maksulaitosluvan. Coinmotion Oy:n tytäryhtiö Prasos Cash Management Oy, jonka toiminta alkoi joulukuussa 2013, ylläpitää Bittimaatti-verkostoa, joka on pohjoismaiden suurin Bitcoin-automaattiverkosto (Brade 2020).

NorthCrypto Oy ylläpitää suomalaista Northcrypto.com-välityspalvelua, joka on osittain EU:n rahoittama. Northcrypto.com tarjoaa Coinmotionin tavoin kryptovaluuttojen osto- ja myyntipalveluita. (Northcrypto 2022.) Sekä Coinmotion että Northcrypto mahdollistavat yritystilien rekisteröinnin alustoillaan.

Kolmannen osapuolen välitys- ja säilytyspalvelut eivät tuo samanlaista turvaa kuin yksityisavainten oma säilyttäminen. Tuore esimerkki on Celsius-lainapalvelu, joka oli sijoittanut asiakkaiden varoja korkeariskisiin kohteisiin saadakseen varoille lisätuottoa. Kesäkuussa 2022 Celsius jäädettiin yllättäen asiakkaiden ulosmaksut ja heinäkuussa Celsius hakeutui konkurssiin. Suomalaiset kauppapaikat ovat kuitenkin turvallisia vaihtoehtoja (Bitcoinkeskus.com 2022).

Suomalaisia kryptovaluuttatoimijoita sääntelee laki virtuaalivaluutan tarjoajista (572/2019), joka on seuraus 5. rahanpesudirektiivin kryptovaluuttatoimijoiden rekisteröintivaatimuksesta. Lisäksi kryptovaluuttatoimiala on säännelty rahanpesulailla sekä Finanssivalvonnan ohjeilla ja määräyksillä. Sääntely ei kuitenkaan tuo sijoittajansuojaa toimialalle eikä Euroopan laajuista yhtenevää sääntelyä vielä ole. (Coinmotion 2021.)

Rahanpesulait edellyttävät asiakkaan tunnistamista ja henkilöllisyyden todentamista. Yritysasiakkaiden kohdalla tämä tarkoittaa myös yrityksen edustajien ja tosiasiallisten edunsaajien henkilöllisyyden tunnistamista. Näiden lisäksi pitää selvittää asiakkaan, tosiallisen edunsaajan ja näiden lähipiirin PEP-status, eli onko heillä poliittista vaikutusvaltaa. Varsinaisen toiminnan osalta asiakasta täytyy jatkuvasti seurata ja liiketoiminnan varojen alkuperää täytyy selvittää. (Coinmotion 2021.)

Northcrypton asiakkaiden varat ovat NorthCrypto Oy:n toimitusjohtajan Ville Runolan mukaan kirjanpidossa varallisuutta, joihin yrityksellä ei ole oikeutta. Varat auditoidaan joka vuosi tilintarkastuksen yhteydessä ja Northcrypto ei käytä kolmannen osapuolen korkopalveluita tuoton hankkimiseksi. Coinmotion toimii samoilla periaatteilla sillä erolla, että Coinmotion tarjoaa asiakkailleen myös erillistä korkotiliä. Coinmotionin kumppani korkopalveluissa on suomalainen Tesseract, joka myös on Finanssivalvonnan reguloima yritys. (Bitcoinkeskus.com 2022.)

Coinmotion ja Northcrypto turvaa asiakkaiden varoja Multisig-kylmäsäilytyksessä. Palvelussa säilytetään vain pieni osa asiakkaiden varoja, joita tarvitaan kaupankäynnissä ja päivittäisissä siirroissa. Jos palvelussa olevia varoja ei ole tarpeeksi, niin Multisig-kylmäsäilytyksestä voidaan nopeasti siirtää manuaalisesti tarvittavia varoja palveluun. (Bitcoinkeskus.com 2022.)

Coinmotion tarjosi välillisesti Tesseract Group Oy:n korkotilipalvelua käyttäjilleen vuoden 2022 loppupuolelle asti, jolloin Coinmotion väitti Tesseractin jakaneen virheellistä tietoa liittyen Tesseractin korkotilipalveluun liittyen. Coinmotionin mukaan heidän ja Tesseractin välinen yhteistyö oli rakennettu kolmikantamallilla, jossa Tesseract on palvelun tuottaja, Coinmotion palvelun välittäjä ja molemmilla osapuolilla oli omat itsenäiset velvollisuudet loppukäyttäjää kohtaan. Toimintamalli oli myös Coinmotionin mukaan kommunikoitu kirjallisesti Finanssivalvonnan joulukuussa 2019. Marraskuussa 2022 Tesseract ilmoitti Coinmotionille kesäkuussa 2022 syntyneistä luottotappioista ja oli näin toiminut Coinmotionin mielestä vastuuttomasti ja lain vastaisesti tarjoten vielä korkopalvelua normaalisti luottotappioiden syntymisen

jälkeen. Coinmotionin sopimuksen mukaan Tesseractin piti hyväksyttää kirjallisesti Coinmotionilla kaikki uudet vastapuolet ja Tesseractin kohtaamissa luottotappiotapahtumissa käytettyjä vastapuolia ei ollut hyväksytetty Coinmotionilla. Coinmotion teki poliisille tutkintapyyntöä Tesseractin toimista. (Coinmotion 2022.)

Poliisi uutisoi helmikuussa 2023, että he eivät aloita esitutkintaa Tesseract Group Oy:n toiminnasta. Poliisin mukaan Tesseractille aiheutuneet luottotappiot johtuivat kryptovaluuttalalla toimineiden yritysten maksuvaikeuksien ja konkurssien aiheuttamasta ketjureaktiosta. Tapahtumat eivät olleet sillä tavoin ennakoitavissa poliisin mukaan, että Tesseractin toimijoita olisi syytä epäillä tahallisesta rikoksesta. Poliisin uutisessa ei kuitenkaan otettu kantaa Coinmotionin ja Tesseractin väliseen sopimukseen, joka velvoitti hyväksyttämään kaikki uudet vastapuolet, jota Coinmotionin mukaan ei ollut tehty. (Poliisi 2023.)

Suomalaisten välityspalveluiden lisäksi kryptovaluuttakauppoja voi tehdä ulkomaalaisissa kryptovaluuttapörssseissä. CoinMarketCap (2023b) on pisteyttänyt kaikki kryptovaluuttapörssit sivuston kävijäliikenteen, keskiarvolikviditeetin, volyymin sekä pörssin ilmoittaman volyymin luotettavuuden perusteella. Tämän perusteella kymmenen eniten pistettä saaneet pörssit, joissa voidaan käydä kauppaa euroilla, ovat pisteytysjärjestyksessä Binance, Coinbase Exchange, Kraken, KuCoin, Bitstamp, Bitfinex, OKX, Bybit, bitFlyer sekä Gate.io.

Näistä ulkomaalaisista pörsseistä ainakin Binance tukee suomalaisia yritystilejä. Binancen (2018) palveluun pystyy rekisteröimään yritystilin valitsemalla etusivulta ”Sign up with Email or Phone” ja sen jälkeen ”Sign up for an entity account”. Tämän jälkeen syötetään yrityksen nimi ja valitaan ”Legal Form of Your Entity”-pudotusvalikosta ”Limited Liability Company”, jos kyseessä on suomalainen osakeyhtiö. Tämän jälkeen syötetään yrityksen sähköpostiosoite, joka ei voi olla ennestään rekisteröity henkilökohtaiselle tilille Binancessa, sekä salasana. Viimeiseksi pyydetään vielä aktivoimaan kaksivaiheinen todennus. Kun rekisteröityminen on suoritettu, pyydetään vahvistamaan tili lähettämällä lisätietoja yrityksestä sekä asiakirjoja, jotka vaihtelevat maan ja yhteisötyypin mukaan. Näihin kuuluvat muun muassa yrityksen pääasialliset edunsaajat, yrityksen pääkäyttäjän tiedot sekä selvitys yrityksen tulonlähteistä. On huomioitava kuitenkin, että suomenkielisiä asiakirjoja ei pysty ainakaan toistaiseksi lähettämään Binanceen. Ruotsi on kuitenkin tuettujen kielten luettelossa englannin lisäksi, joten ruotsinkielisten asiakirjojen toimittaminen pitäisi oletettavasti olla helpompaa, kuin virallisten käännösten hankkiminen notaarin vahvistamana. (Binance 2018.)

Keskitettyjen pörssi- ja välityspalveluiden lisäksi löytyvät myös P2P-palveluja, eli palveluja, joissa pystyy tekemään kauppaa suoraan muiden henkilöiden kanssa. Yksi pitkään toiminut P2P-palvelua tarjoava yritys oli suomalaistaustainen LocalBitcoins Oy. LocalBitcoins oli vuonna 2012 perustettu Bitcoin-kaupankäyntisivusto, jossa eri ihmiset eri maista pystyivät vaihtamaan muiden kanssa paikallista fiat-valuutta Bitcoinneiksi. Sivusto antoi käyttäjien luoda

ilmoituksia, joissa he pystyivät valitsemaan maksutavan ja valuuttakurssin Bitcoinien ostamiseksi muilta käyttäjiltä sekä myymiseksi muille käyttäjille. (LocalBitcoins 2022.) LocalBitcoins tarjosi turvallisimpien kauppojen saavuttamiseksi muun muassa escrow-palvelun, eli he pitivät hallussaan molempien osapuolten varat, kunnes kauppa oli molempien osalta suoritettu. (Karamé & Androulaki 2016, 146.) LocalBitcoins ei ollut kuitenkaan keino suorittaa kryptovaluuttakauppoja nimettömästi, vaan regulaatio oli tuonut myös heille KYC-prosessit asiakkaidensa tunnistamiseksi (LocalBitcoins 2019). Alkuvuonna 2023 LocalBitcoins ilmoitti lopettavansa palvelunsa yli 10 vuoden toiminnan jälkeen ilman mitään suurempia ongelmia taustalla, kuin pitkään jatkunut huono markkinatilanne (LocalBitcoins 2023).

### 2.2.9 Lompakot

Laitelompakot ovat laitteita, jotka säilyttävät sisällään yksityisavaimet ja tarjoavat apukeinoja kryptovaluuttatransaktioille. Markkinoilla on useampia laitelompakkovalmistajia, joista tunnetuimpia ovat Trezor ja Ledger. Nämä molemmat ovat erittäin turvallisia ja sertifioituja torjumaan erilaisia fyysisiä ja loogisia hyökkäyksiä. Laitelompakoidenkin tapauksessa tulisi varmuuskopioida yksityisavaimet esimerkiksi kirjoittamalla ylös muistitekniset sanat paperille siltä varalta, että laitelompakko katoaa, varastetaan tai rikkoontuu. Laitelompakon tuoman turvallisuuden ja ohjelmistopohjaisen lompakon, pörssi- tai välityspalvelun tuoman kaupan-teen helppouden yhdistelmä voi vähentää riskejä kryptovaluuttojen menettämiseksi. (Karamé & Androulaki 2016, 147.)



Kuvio 1: Laitelompakot Coldcard Mk3, Ledger Nano X, Trezor Model T, KeepKey ja BitBox02 (Costea 2019)

Trezorilla on kaksi laitelompakkoa myynnissä tällä hetkellä: Model T ja Model One. Model T on kalliimpi versio, jossa on halvempaan Model Oneen verrattuna isompi värinäyttö, USB-C-liitin, tuki useammalle kryptovaluutalle ja tokenille sekä mahdollisuus peittää transaktioita

CoinJoin-teknologialla. Trezor Model T:ssä pystyy lisäksi luomaan Shamir's secret-share varmuuskopio-osuuksia, niin kuin luvussa 2.2.3 olen kuvaillut, sekä ottamaan käyttöön moniallekirjoitukset. (Trezor 2023.)

Toinen suosittu laitelompakkovalmistaja on Ledger. Ledgerillä on kolme laitelompakkoa myynnissä, jotka ovat hintajärjestyksessä kalliimmasta halvimpaan Stax, Nano X ja Nano S Plus. Ledger Stax on uusi malli, joka on hintaluokassaan samanhintainen kuin Trezor Model T, mutta jossa on kaareva E Ink -kosketusnäyttö ja langaton latausmahdollisuus. Ledger Stax ja Nano X ovat varustettuja Bluetooth-yhteydellä, joita voi käyttää helposti älypuhelimella. Kaikki Ledger-laitelompakot ovat myös varustettuja USB-C-liittimellä, jolla lompakot saa helposti kytkettyä tietokoneeseen. Ledgerit tukevat myös yli 5000 kryptovaluuttaa, tokenia ja NFT:tä. (Ledger 2023a.) Trezorin ja Ledgerin laitelompakoista on hyvin vaikea suositella yhtä voittajaa, koska lompakoiden hinnat vaihtelevat 57 eurosta 279 euroon ja ominaisuudet sen mukaan, eli riippuu hyvin pitkälti käyttötarkoituksesta ja säilytettävistä kryptovaluutoista.

Yksi keino siirtää taholta toiselle esimerkiksi bitcoineja fyysisesti ja turvallisesti on Opendime-avaimet. Opendime-avaimet ovat pieniä USB-tikkuja, jotka ovat suojattu väärentämiseltä ja niiden sisältämä saldo voidaan varmentaa nopeasti. Näiden käyttö toisaalta vaatii sen, että molemmat osapuolet ymmärtävät, miten nämä avaimet toimivat. Opendime-avaimet voidaan antaa toiselle taholle ilman että siirto merkitään lohkoketjuun, ja vastaanottaja voi sitten esimerkiksi nostaa saldon toiseen lompakkoon. (Ammous 2019, 396.) Tätä kirjoittaessa kolmen Opendime-avaimen paketti maksaa 69 Yhdysvaltain dollaria ilman postituskuluja, joten Opendime ei luultavasti sovi ihan pienimpien maksujen maksamiseen toiselle osapuolelle (Opendime 2022).

Ohjelmistopohjaisten lompakoiden ei tarvitse säilyttää koko lohkoketjua, tämä olisi muuten kohtuutonta ainakin Bitcoinin tapauksessa, jossa lohkoketjun koko on tätä kirjoittaessa yli 455 gigatavua (YCharts 2023), jolloin älypuhelimessa toimivat lompakkosovellukset eivät olisi enää käytännöllisiä. Tätä varten Bitcoin-verkossa pystyy myös tehdä yksinkertaistettuja transaktiovarmennuksia, jolloin ohjelma varmentaa ainoastaan rajoitetusti esimerkiksi lohkokoon ja transaktion olemassaolon Merkle-puussa sekä lähettää transaktion varmennusta varten Bitcoin-noodeille. Tällä hetkellä yksinkertaistetut ohjelmat kuitenkin yhdistävät ainoastaan neljään Bitcoin-noodiin, vähentäen hajautusta verkossa, jolloin myös turvallisuus heikentyisi, jos kaikki neljä noodia olisivat pahansuopia. (Karame & Androulaki 2016, 125-126.)

Hajautetuilla ohjelmistopohjaisilla lompakoilla on julkinen ja yksityinen salausavain, niin kuin esimerkiksi Bitcoin-lompakoillakin, ja varmuuskopiointi toimii myös kirjoittamalla ylös muistitekniset sanat. Käytännössä ohjelmistopohjaiset lompakot saavat kuitenkin vain pienen osan lohkoketjun transaktioista, jotka yhdistetyt noodit suodattavat niille. Noodien tehtäväksi jää varmentaa transaktioiden allekirjoitukset, varmentaa louhitut lohkot sekä varmentaa, että

transaktiot sisältyvät vastaanotettujen lohkojen Merkle-puussa. (Karame & Androulaki 2016, 126.)

Älypuhelimissa toimivat lompakkosovellukset tuovat paljon helpotusta nopeaan maksamiseen esimerkiksi NFC-teknologian tai QR-koodien avulla. Älypuhelinsovellukset myös tallettavat yksityiset avaimet turvallisesti puhelimen muistiin, jolloin transaktioita voi varmentaa nopeasti esimerkiksi sormenjäljellä tai PIN-koodilla. (Karame & Androulaki 2016, 147.)

Exodus on suosittu ohjelmistolompakko sekä tietokoneelle desktop-versiona että älypuheliin. Näiden lisäksi Exoduksella on myös Web3-lompakko, joka toimii selainlaajennuksena ja joka tukee useampaa lohkoketjua. Saman lompakon pystyy synkronoimaan kaikille alustoille, joten Exodus sopii hyvin sellaiselle, joka haluaa käyttää samaa lompakkoa sekä tietokoneellaan että puhelimessaan. Exoduksen lompakossa pystyy myös steikkaamaan useampia kryptovaluuttoja natiivisesti ilman tarvetta siirtää varoja lompakosta ulos. (Exodus 2023a.)

Exodus lompakko on myös yhteensopiva Trezorin laitelompakoiden kanssa. Tämä tuo esimerkiksi PoS-steikkauksen mahdolliseksi Trezorissa säilytetyille PoS-kryptovaluutoille, kun tätä ominaisuutta ei löydy natiivisesti Trezorista. (Exodus 2023b.) Ledgerin Ledger Live -sovelluksella pystyy natiivisestikin steikkaamaan Ledgerissä säilytettäviä PoS-kryptovaluuttoja (Ledger 2023b).

Suurin osa ohjelmistopohjaisista lompakoista on useampia kryptovaluuttoja tukevia. Yleensä sovelluksen verkkosivustolla on lueteltu myös tuetut kryptovaluutat ja tokenit, joten ohjelmistolompakon voi helposti valita sen mukaan, mitä kryptovaluuttaa tarvitsee säilyttää. Jos vaihtoehtoja kuitenkin on liikaa, niin on suositeltavaa lukea esimerkiksi sovelluksen saamia arvosteluja tai etsiä hakukoneella, onko sovelluksesta löytynyt esimerkiksi korjaamattomia haavoittuvuuksia. (Bédrune & Guillemet 2021.)

Ohjelmistolompakoiden lisäksi on olemassa erilaisia online-lompakoita, eli käytännössä palveluja, jotka säilyttävät verkossa kryptovaluuttoja, mutta tässä tapauksessa palveluntarjoajalla ei ole pääsyä varoihin, vaan yksityisavain säilytetään palveluntarjoajan palvelimella ja käyttäjällä on suora pääsy varoihinsa. Tämä on kuitenkin erittäin turvaton keino säilyttää kryptovaluuttavaroja verrattuna esimerkiksi laitelompakoihin tai muihin offline-lompakoihin, enkä aio sen takia luetella yhtäkään esimerkkiä online-lompakosta. (Karame & Androulaki 2016, 148-149.)

Laite- ja ohjelmistopohjaisten lompakoiden lisäksi on mahdollisuus luoda esimerkiksi Bitcoin-paperilompakko. Koska paperilompakkoita ei säilytetä digitaalisesti missään palvelussa tai verkkoon kytketyssä tietokoneessa, eivät niitä myöskään voi varastaa hakeroimalla tietokoneen tai muun laitteen. Tämä tuo huomattavan edun muihin vaihtoehtoihin, koska vaikka joku kryptovaluuttapalvelu tai -sovellus toimisi toistaiseksi moitteettomasti, se ei takaa sitä, ettei

tulevaisuudessa löytyisi haavoittuvuuksia, joita rikolliset hyödyntävät. Kun kryptovaluuttavaroja on kerran siirretty lompakosta ulos, niitä ei todennäköisesti pysty enää koskaan palauttamaan. Toisaalta jos paperilompakko kuitenkin tuhoutuu tai häviää, ei sen sisältäviä varoja pystytä myöskään palauttamaan. (Karamé & Andrólaki 2016, 149.)

Suosituin keino luoda paperilompakko on BitAddress-generaattorilla, joka käyttää selaimen omaa Javascript-moottoria, eli lompakko luodaan paikallisesti käyttäjän omalla koneella. BitAddress-generaattorissa liikutetaan hiirtä tai kirjoitetaan satunnaisia merkkejä tekstikenttään luodakseen mahdollisimman satunnaista syötettä, kunnes generaattori ilmoittaa, että merkkejä on riittävästi. Tämän jälkeen valitaan minkä tyyppisen lompakon halutaan luoda ja tulostetaan paperilompakko. Kyseinen keino sisältää itsessään kuitenkin riskejä: yksityisavain voi vuotaa, jos joku on hakkeroinut koneelle ja nähnyt työpöydän sisällön, jos joku on hakkeroinut generaattorisivuston tai jos joku on päässyt käsiksi tulostimen välimuistiin. Keinoja ennaltaehkäistä äsken mainittuja riskejä on luoda paperilompakko tietokoneella, jota ei ole kytketty verkkoon, ja mieluiten live-käyttöjärjestelmällä. Live-käyttöjärjestelmä, esimerkiksi Ubuntu Live, ei talleta tehtyjä muutoksia kovalevylle muistiin. Vielä turvallisempi keino kuin paperilompakon käyttäminen on kuitenkin käyttää laitelompakkoa, kuten Trezoria tai Ledgeriä. (Cryptonews 2023.)

### 2.3 Yritysturvallisuus ja riskienhallinta

Elinkeinoelämän keskusliitto (2022) EK kertoo yritysturvallisuudesta seuraavasti: ”Yritysturvallisuuden keskeinen tehtävä on edistää yrityksen kilpailukykyä ja parantaa tuottavuutta. Turvallisuusjohtaminen on osa normaalia yrityksen johtamista. Tavoitteena ei ole erillinen turvallisuustoiminto, vaan yrityksen toiminnan jatkuvuuden, turvallisuuden ja vaatimustenmukaisuuden varmistaminen kaikissa tilanteissa, luonnollisena osana yrityksen riskienhallinnan kokonaisuutta.”



Kuvio 2: EK:n yritysturvallisuusmalli (Elinkeinoelämän keskusliitto 2022)

Keskeisiä osa-alueita yritysturvallisuusmallissa (Elinkeinoelämän keskusliitto 2022), joihin kryptovaluuttojen turvallisuus liittyy, ovat tietoturvallisuus, väärinkäytösten ja poikkeamien hallinta sekä tuotannon ja toiminnan turvallisuus. Seuraavissa alaluvuissa avaan riskienhallintaa sekä riskejä, jotka erityisesti liittyvät tietoturvaan ja paloturvallisuuteen.

### 2.3.1 Riskienhallinta

Riskienhallinta on ISO 31000 (2018) -standardin mukaan osa organisaation hallintatapaa ja johtajuutta. Riskienhallinta on olennainen osa kaikkia organisaatioon liittyviä toimintoja ja riskienhallinnassa otetaan huomioon organisaation sisäinen ja ulkoinen toimintaympäristö, johon sisältyy ihmisten käyttäytyminen ja kulttuuriset tekijät. Riskienhallintaa kehitetään jatkuvasti organisaatiossa oppimisen ja kokemuksen myötä.

Organisaation ylimmän johdon ja hallituksen olisi varmistettava ISO 31000 (2018) -standardin mukaan, että riskienhallinta sisällytetään organisaation kaikkiin toimintoihin. Ylimmän johdon ja hallituksen tulisi osoittaa johtajuutta ja sitoutumista laatimalla toimintaperiaatteet, jossa määritellään riskienhallinnan suunnitelma, toimintatapa tai -malli. Ylimmän johdon tulisi myös varmistaa, että koko organisaation riskien hallintaan varataan tarvittavat resurssit, sekä nimetä riskienhallinnasta vastaavat ja riskienhallintaan valtuutetut tahot organisaation eri tasoilla, eli riskien omistajat.

Riskienhallintaprosessi on iteratiivinen prosessi, joka on oltava osa johtamista ja päätöksentekoa. Sitä voidaan soveltaa operatiivisella, strategisella, projektin tai ohjelman tasolla. Prosessi voidaan räätälöidä tavoitteiden saavuttamiseksi. Ihmisten käyttäytyminen ja kulttuurin muuttuva luonne olisi huomioitava riskienhallintaprosessin kaikissa vaiheissa. (ISO 31000 2018.)

Organisaation tulisi määrittää riskitason, eli kriteerit, kuinka paljon ja minkä tyyppisiä riskejä organisaatio voi tai ei voi ottaa. Organisaation tulisi myös määrittää kriteerit, joilla arvioidaan riskin merkittävyyttä ja jotka tukevat päätöksentekoprosessia. Riskien arviointi on kokonaisvaltainen prosessi, joka kattaa ISO 31000 (2018) -standardin mukaan riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin.

Riskien tunnistamisen tarkoitus on löytää, havaita ja kuvata riskit, jotka voivat auttaa tai estää organisaation tavoitteiden saavuttamista. Riskianalyysin tarkoitus on ymmärtää riskin luonne, sen ominaisuudet sekä riskitaso. Riskianalyysi on lähtökohta riskin merkityksen arvioinnille ja päätöksille siitä, millä keinoin riski tulisi käsitellä, jos sitä tarvitsee käsitellä. Riskien merkityksen arviointiin kuuluu riskianalyysin tulosten vertaaminen määriteltyihin riskikriteereihin. Arvioinnin perusteella voidaan päättää olla tekemättä muita toimenpiteitä, tarkastella riskien käsittelyn vaihtoehtoja, tehdä lisäanalyysieja pyrkimyksenä ymmärtämään riskiä paremmin, ylläpitää nykyisiä hallintakeinoja tai harkita tavoitteita uudelleen. (ISO 31000 2018.)

Riskien käsittely on toistuva prosessi, johon kuuluvat riskien käsittelyn vaihtoehtojen kehittäminen ja valinta, suunnittelu ja toteuttaminen, vaikuttavuuden arviointi sekä päätös siitä, onko jäljelle jäävä riski hyväksyttävällä tasolla ja riskin käsittelyn jatkaminen, mikäli jännösriski ei ole hyväksyttävällä tasolla. Riskinkäsittelytapoja voivat olla riskin torjuminen, ottaminen, lisääminen, lähteen poistaminen, todennäköisyyden muuttaminen, seurausten muuttaminen, jakaminen tai säilyttäminen. Riskien käsittely voi myös aiheuttaa uusia riskejä, joita täytyy hallita. (ISO 31000 2018.)

### 2.3.2 Tietoturva

ISO 27000 -standardin (2020) mukaan tietoturvan pyhään kolminaisuuteen kuuluvat tiedon luotettavuus, eheys sekä saatavuus. Organisaation liiketoiminnan kannalta tieto tulee suojata asianmukaisesti. Tietoturvallisuuden tarkoituksena on varmistaa liiketoiminnan jatkuvuus ja pitää tietoturvahäiriöiden seuraukset vähäisinä. Tietoturvallisuuden hallintakeinot täytyy määritellä ja niitä täytyy valvoa, katselmoida ja parantaa tarvittaessa, jotta organisaation turvallisuustavoitteet saavutetaan varmasti.

Tietoturvariskit täytyy ISO 27000 -standardin (2020) mukaan arvioida ja tämän pitäisi sisältää riskien analyysin sekä riskien vaikutusten arvioinnin. Tietoturvallisuus saavutetaan toteuttamalla hallintakeinot, jotka ovat valittu riskien hallintaprosessin avulla.

Katakri (2020, 5-6) on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää yritysten turvallisuusjärjestelyjen arviointityökaluna. Katakriin on koottu kansallisiin säästöihin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset tietoturvalle. Vaikka Katakriin keskeisimmät auditointimenetelmät ovatkin luotu kansainvälisten ja kansallisten turvaluokiteltujen tietojen turvallisuuden auditointia varten, niin se soveltuu hyvin myös arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista. Katakri on laadittu normaaliolojen toiminnan työkaluksi, eikä siinä käsitellä poikkeusolojen erillissuunnitelmia.

Organisaation johto vastaa Katakriin (2020, 9) mukaan siitä, että organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat tietoturvaluustoimenpiteiden kytkeytymistä organisaation toimintaan. Periaatteet voidaan kuvata esimerkiksi yksittäisenä dokumenttina, osana yleistä toimintaperiaatetta, politiikkaa tai strategiaa ja ne ovat tietojen suojaamisen kannalta kattavat sekä tarkoituksenmukaiset. Katakriin (2020, 11) mukaan organisaation pitäisi arvioida olennaiset tietoturvariskit samalla tavalla kuin muitakin organisaation riskejä sekä mitoittaa tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti.

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamista siten, että estetään luvaton pääsy tietoihin. Luvaton pääsy estetään varmistamalla, että tietoja käsitellään ja säilytetään asianmukaisesti, mahdollistamalla henkilöiden pääsy tietoihin tarpeen perusteella, ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet sekä estämällä oikeudetta tapahtuva tunkeutuminen. (Katakri 2020, 22-24.)

Tietoturvariskien arvioinnissa tulisi ottaa huomioon pääsyoikeuksien hallintaan ja muihin turvallisuusprosesseihin sisällytettävät tiedonsaantitarpeet, tehtävien eriyttämisen ja vähimpien oikeuksien periaatteet (Katakri 2020, 25). Tietoja on käsiteltävä siten, että pääsy estetään sivullisilta ja henkilöiltä, joilla ei ole tiedonsaantitarvetta. Suora näkö- ja kuuloyhteys on esitettävä tietoon sekä tietoa sisältävä päätelaite, eli tietojärjestelmää, jota henkilö käyttää työtehtäviensä hoitamiseen, on säilytettävä turvallisesti. (Katakri 2020, 29.)

Käyttöoikeuksien hallinnan keskeinen tavoite on varmistua siitä, että vain oikeutetuilla käyttäjillä on pääsy suojattavaan tietoon. Käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja tarpeettomat tunnukset poistetaan välittömästi. Tarpeettomat laajat oikeudet mahdollistavat myös hyökkääjälle tarpeettoman laajat toimintamahdollisuudet. Käyttöoikeudet tulisi tämän takia rajata vähimpien oikeuksien periaatteen mukaisesti. Pääsyoikeuden ajantasaisuutta voidaan varmistaa esimerkiksi katselmoimalla kaikkien käyttäjien pääsyoikeuksia säännöllisin väliajoin. (Katakri 2020, 75.)

Hyvä turvallisuuskäytäntö käyttäessä tietojärjestelmiä tai esimerkiksi kolmannen osapuolen kryptovaluuttapalveluja on käyttää monivaiheista tunnistautumista (engl. multi-factor authentication tai MFA). Tunnistautumisvaiheiksi luetellaan yleensä jotain mitä tiedät (esimerkiksi salasana tai PIN-koodi), jotain mitä sinulla on (esimerkiksi sovelluksen kertakoodi tai tunnistuslaite) tai jotain mitä olet (esimerkiksi sormenjälki). (Kyberturvallisuuskeskus 2022.)

Kertakäyttökoodoja (engl. one-time password tai OTP) varten on olemassa sovelluksia, kuten Google Authenticator tai Authly, joka luo aikaan perustuvan 6-numeroisen koodin. Tämä on huomattavasti turvallisempi vaihtoehto kuin palvelun lähettämä kertakäyttökoodi tekstiviestinä. Sormenjälki voidaan todentaa älypuhelimien sormenjälkilukijalla. Salasana tai PIN-koodi pitäisi olla vain yhdellä henkilöllä tiedossa. Näiden kaikkien vaiheiden yhdistelmä luo turvallisen käyttöympäristön kaikissa järjestelmissä, jossa MFA on mahdollista ottaa käyttöön. Näin ollen kannattaa aina ottaa esimerkiksi kolmannen osapuolen palveluissa monivaiheinen tunnistautuminen käyttöön, jossa palvelu mahdollistaa sen käyttämisen. (Kyberturvallisuuskeskus 2022.)

## 2.4 Kirjanpito

Yhtiön vastaanottaessa ja lähettäessä maksuja kryptovaluuttoina kaikki tuotot ja kulut kirjataan euromääräisinä kirjanpitoon tapahtumahetken kurssilla. Luovuttaessa kryptovaluutoista, esimerkiksi maksaessa kuluja niillä tai myydessä niitä, kirjataan tuloslaskelman rahoitustuotot tai -kulut tileille hankinta- ja luovutushetken välinen kurssiero. Tilikauden aikana kryptovaluutat ovat taseessa tase-erässä rahoitusarvopaperit ja tilillä muut arvopaperit. (Coinmotion 2021.)

Kun yhtiö haluaa sijoittaa kassareservejä kryptovaluuttaan esimerkiksi inflaationsuojaa varten vaikuttaa sijoitushorisontti omaisuuslajin valintaan, eli merkitäänkö omaisuuslaji taseeseen pysyviin vai vaihtuviin vastaaviin. Jos tarkoituksena on sijoittaa kryptovaluuttoihin monena peräkkäisenä tilikautena, voidaan omaisuuslaji merkitä pysyviin vastaaviin sijoitukset-erään, mutta lähtökohtaisesti kuitenkin rahoitusarvopaperit-erään. (Coinmotion 2021.)

PoW-louhintatulot kirjataan sen tilikauden tuloksi, jolloin kryptovaluutta on vastaanotettu. PoS-tulot jaksetetaan tasaisesti sen jakson ajalle, kun kryptovaluutta on ollut kiinnitettynä. Louhinnasta syntynyt omaisuuslaji ratkaistaan tapauskohtaisesti, onko omaisuuslaji vaihto-omaisuutta vai rahoitusomaisuutta. (Coinmotion 2021.)

Rahoitusarvopaperit- ja vaihto-omaisuus-erään kirjatut kryptovaluutat esitetään tilinpäätöksessä todellisen hankintamenon tai sitä alemman arvon mukaan. Pysyviin vastaaviin kirjatut kryptovaluutat esitetään todellisen hankintamenon mukaan. Rahoitusarvopaperit-erään ja pysyviin vastaaviin kirjattujen kryptovaluuttojen arvonalentuma kirjataan rahoituskuluihin, kun taas vaihto-omaisuuteen kirjattu arvonalentuma kirjataan varaston muutoksena. Tilinpäätöksen liitetietona esitetään lisäksi tarvittavat tiedot arvostusmenetelmistä oikean ja riittävän kuvan antamiseksi. On myös perusteltua antaa liitetiedoissa kryptovaluuttojen kokonaismäärät, kun tieto on olennaista. (Coinmotion 2021.)

## 2.5 Verotus

Verotus on myös oleellinen osa muun muassa yrityksen toiminnan jatkuvuuden edellytyksiä. Osakeyhtiö on tuloverolain (1535/1992) 9 § mukaan velvollinen suorittamaan veroa tulon perusteella. Korkeimman hallinto-oikeuden (42/2019) päätöksen mukaan kryptovaluutta on sellaista varallisuutta, joka varallisuusverolain nojalla tulisi pitää verotettavana varallisuutena, eikä sitä voi jättää tuloverolaissa tarkoitetun omaisuuden alan ulkopuolelle. Yritys tulee noudattaa voimassa olevia verosäädöksiä ja maksaa veroja myös kryptovaluuttojen osalta. Verotuksen laiminlyönnillä voi olla vakavat seuraamukset niin osakeyhtiölle, kuin myös osakeyhtiön päättävällä elimellä.

Kryptovaluuttojen realisoitu arvonnousu, esimerkiksi sitä myydessä tai vaihdettaessa toiseen kryptovaluuttaan, on yritykselle veronalaista tuloa. Arvonlaskun verovähennysoikeus riippuu siitä, mihin omaisuuslajiin kryptovaluutta kuuluu yhtiön taseessa. (Coinmotion 2021.)

Laki elinkeinotulon verottamisesta (360/1968) 14 §:n 2 momentin mukaan vaihto-omaisuuden hankintamenon suuruus määritetään FIFO-periaatteen (First In, First Out) mukaan, eli ”olettaen, että samanlaiset hyödykkeet on luovutettu tai kulutettu siinä järjestyksessä, missä ne on hankittu”. Rahoitusomaisuuden ja muun omaisuuden hankintameno määritetään todellisen hankintamenon perusteella yksilöllisesti (Coinmotion 2021).

## 3 Opinnäytetyön tutkimusmenetelmälliset ratkaisut

Olen valinnut opinnäytetyön menetelmällisiin ratkaisuihin kvalitatiivista tutkimusta ja puolistrukturoitua teemahaastattelua. Teemahaastattelu valikoitui sen takia, että Anita Saaranen-Kauppinen ja Anna Puusniekan (2006) mukaan menetelmä sopii hyvin sellaisiin tilanteisiin,

jolloin halutaan tietyistä asioista tietoa, eikä haluta antaa haastateltaville liian suuria vapauksia haastattelutilanteessa. Kvalitatiiviseen tietoperustaan kuuluu kryptovaluuttoihin liittyvät painetut ja sähköiset lähteet. Puolistrukturoidussa teemahaastattelussa olen haastatellut kryptovaluuttoihin erikoistuneita asiantuntijoita.

Kvalitatiivisella, eli laadullisella menetelmällä, keskitytään enemmän pienemmän ryhmän haastatteluun, jolloin kysymykset voivat vaihdella ja tutkimuksesta voidaan näin tehdä hieman yksityiskohtaisempi ja räätälöidympi. Laadullisessa tutkimuksessa tutkija yleensä haluaa osallistua tutkittavien toimintaan, jolloin tutkija pääsee lähelle tutkittavia. (Moilanen, Ojasalo & Ritalahti 2015, 105.)

Teemahaastattelu sijoittuu rakenteellisesti lomakehaastattelun ja avoimen haastattelun väli-maastoon. Teemahaastattelu ei etene tarkkojen, yksityiskohtaisten ja valmiiksi muotoiltujen kysymysten kautta, vaan se ohjailee haastateltavaa haluttuun suuntaan, mutta jättää reilusti tilaa haastateltavan omille ajatuksille. Teemahaastattelu kuitenkin on astetta strukturoidumpi kuin avoin haastattelu, sillä siinä tehdyn tietoperustan pohjalta luodut aihepiirit ja teemat ovat kaikille haastateltaville samoja, vaikka niissä liikutaankin joustavasti ilman tiukkaa etenemisreittiä. (Saaranen-Kauppinen & Puusniekka 2006.)

Teemahaastattelu on keskustelunomainen tilanne, jossa käydään läpi ennalta suunniteltuja teemoja ja aihepiirejä. Haastattelut eivät koskaan ole täysin samanlaisia, ja eri haastateltavien kanssa voidaan käsitellä eri teemoja eri laajuuksilla. Haastattelijalla ei ole haastattelussa mukanaan runsaita muistiinpanoja, jotta haastattelija voi keskittyä itse keskusteluun. Haastattelun teemoja sekä joitain apukysymyksiä voi käyttää haastattelun apuna, kunhan haastattelu ei ole pikkutarkkojen, valmiiksi laadittujen kysymysten esittämistä. (Saaranen-Kauppinen & Puusniekka 2006.)

Haastattelun etuna on haastateltavan oma kokemus ja tietotaito, joka itsessään on riittävä informaatio aiheesta tutkimusta varten. Haastattelun haittana voidaan pitää, että menetelmällä ei saada tilastollista objektiivista tietoa.

### 3.1 Haastattelupohjan laatiminen

Haastattelupohja on laadittu harkitsemalla tarkkaan seuraavia tutkimuskysymyksiä, käyttäen pohjana tietoaaineistoa:

- Miten voidaan käsitellä ja säilyttää kryptovaluuttoja turvallisesti osakeyhtiössä, jossa on useampi osakas?
- Mitkä ovat hyviä toimintatapoja kryptovaluuttojen käsittelemiselle, jos usean osakkaan osakeyhtiössä osakas menehtyy tai yksityisavain katoaa?

- Millä tavoin osakeyhtiö voisi ansaita tuottoa kryptovaluuttaomistuksilleen tai hyödyntää louhimista?

Tarkoituksena oli saada vastaus tutkimuskysymyksiin asiantuntijoilta. Tutkimuskysymysten lisäksi oli toivottavaa, että asiantuntijat arvioivat myös riskienhallintaan liittyviä kysymyksiä.

Valmistauduin haastatteluihin laatimalla Word-tiedoston, johon yksinkertaisesti luettelin kaikki tutkimuskysymyksiin liittyvät kysymykset, jotka tulivat mieleeni. Teemoitin kysymysaiheet niin, että ehtisin haastattelussa kysyä tasapuolisesti eri teemoihin liittyviä kysymyksiä. En kysynyt kaikkia laatimiani kysymyksiä kaikilta, vaan painotin enemmän sellaisia kysymyksiä sellaisten asiantuntijoiden kohdalla, joilla uskoin olevan enemmän tietoa ja kokemusta tietystä aiheesta kuin muilla. Kysymyksiä en lähettänyt asiantuntijoille etukäteen. Näin saatiin monipuolisempia asiantuntijoiden näkemyksiä kryptovaluuttojen turvallisesta hallinnoinnista. Halusin saada enemmän mielipiteitä ja ehdotuksia kryptovaluuttojen turvallisesta hallinnoinnista yrityksissä, kuin tietoaaineistoa, jota olen jo kerännyt etukäteen. Haastatteluvastaukset löytyvät luvusta 4.1 ja liitteessä 1 olen luetellut käyttämiäni teemakysymyksiä haastatteluisissa.

Haastatteluiden jälkeen osa kysymyksistä jäi pois sen takia, että kysyin kysymystä vain yhdeltä tai parilta asiantuntijalta, vastaus oli jo tullut muissa kysymyksissä tai vastaus ei ollut oleellinen tutkimuskysymyksiä varten. Haastattelu oli myös puolistrukturoitu ja vapaamuotoisempi, joten en kysynyt kysymyksiä tarkalleen niin kuin ne ovat liitteessä 1 kirjoitettuna.

### 3.2 Tutkimusaineiston kerääminen

Haastattelua varten kirjasin itselleni ylös asiantuntijoita, joilla on oman kokemukseni sekä tutkimieni lähteiden mukaan vuosien kokemus kryptovaluutoista, ovat antaneet medialle useita luotettavia haastatteluja aiheesta, ovat tällä hetkellä töissä tai tekevät elämäntyötä kryptovaluuttojen parissa. Minulle tuli monta nimeä mieleen lyhyessä ajassa, joten kirjasin suoraan Excel-tiedostoon asiantuntijoiden nimet, yhteystiedot sekä missä he ovat töissä ja missä asemassa.

Aloin ottamaan yhteyttä mahdollisimman erilaisiin asiantuntijoihin. Kysyin tutkimuslupaa ja kerroin samalla, että haastateltujen nimet tullaan julkaisemaan opinnäytetyössä. Sen jälkeen, kun olin saanut sovittua seitsemän eri asiantuntijan kanssa haastatteluajankohdat päätin, että minulla on tarvittava määrä asiantuntijahaastatteluja sovittuna opinnäytetyötä varten ja sovin lisää haastatteluja, jos jokin jo sovituista haastatteluista peruuntuu. Kaikki seitsemän haastattelua toteutuivat joulukuussa 2022 ja haastateltavilta saatava materiaali alkoi toistaa itseään. Myös erilaisia näkökulmia löytyi, joten uusia haastatteluja ei tarvinnut tuottaa. Toisin sanoen haastattelu aineisto saavutti saturaatiopisteen seitsemän haastattelun jälkeen.

Lopputuloksissa on huomattava, että osa haastatelluista esimerkiksi työskentelee kryptovaluuttapalvelussa tai on kytköksissä sellaisen kanssa. Seuraavassa taulukossa olen kuitenkin esittelyt haastateltujen taustoja, joista voi päätellä haastattelun subjektiivisuutta tai luotettavuutta. Toisin sanoen voidaan väittää, että haastateltavien tausta parantaa tulosten luotettavuutta. Haastattelu oli hyvin valittu tutkimusmenetelmä tähän työhön.

Seuraavana luettelen asiantuntijat aakkosjärjestyksessä esittelyineen. Esittelyt perustuvat haastateltujen omiin sanoihin taustoistaan. Aineistoa kerääntyi yhteensä 6 tunnin ja 20 minuutin edestä, eli keskimäärin noin 54 minuuttia haastattelua kohden.

Jusa Harju (2022)	Harju (2022) työskentelee sivutoimisesti kryptovaluuttojen parissa yrityksen kautta. Harjun (2022) yritys louhii kryptovaluuttoja näytönohjainten avulla. Häntä on aina kiinnostanut tietokoneet ja teknologia. Kryptovaluutat olivat jotenkin tuttuja jo 2010-luvun alkupuolella, mutta 2019 vasta alkoi kiinnostus heräämään niitä kohtaan. Tämän jälkeen hän on alkanut sijoittamaan kryptovaluuttoihin sekä louhimaan niitä.
Pessi Peura (2022)	Peuralla (2022) löytyy kokemusta kryptovaluuttojen parissa yli kymmenen vuoden aikajänteeltä. Alalla hän on työskennellyt yli viisi vuotta. Peura (2022) toteaa itse, että hän on erittäin kokenut aiheesta verraten nuoreen toimialaan. Peura (2022) työskentelee tällä hetkellä Coinmotion Oy:llä Partner Manager -tittelillä, eli hän osallistuu palveluiden kehittämiseen, liiketoiminnalliseen tuotekehitykseen, asiakaspalveluun, asiakastapahtumien järjestämiseen sekä monenlaisiin asiantuntija- ja koulutustehtäviin.
Janne Piironen (2022)	Piirroista (2022) haastattelin Bitcoin-kirjailijan roolissa. Piironen (2022), Jenni Selosmaan ja Toni Heiskasen ”Bitcoin - Rahan vallankumous” -kirja julkaistiin marraskuussa 2022. Hän on myös työskennellyt Avain vapauteen -viikkokirjeen parissa kirjoittaen Bitcoin-aiheisia uutisia ja tietoja. Piironen (2022) on vuodesta 2017 lähtien opiskellut aktiivisesti kryptovaluuttoja.
Ville Runola (2022)	Runola (2022) on touhunnut enemmän tai vähemmän kryptovaluuttojen parissa vuodesta 2013 lähtien. Runola (2022) perusti vuonna 2018 Northcrypton, joka on Suomessa Finanssivalvontaan rekisteröitynyt reguloitu kryptovaluuttojen välityspalvelu. Northcrypto tarjoaa myös

	Private Banking -palveluita korkeamman varallisuuden henkilöille ja yrityksille.
Jenni Selosmaa (2022)	Selosmaa (2022) on yrittäjä ja kirjailija, joka on viimeisten muutaman vuoden aikana kirjoittanut päätoimisesti ”Bitcoin - Rahan vallankumous” -tietokirjaa yhdessä Janne Piironen ja Toni Heiskasen kanssa. Kirja julkaistiin marraskuussa 2022. Muuten Selosmaa (2022) on kauppatieteiden maisteri ja erikoistunut rahoitukseen sekä sillä taustalla tehnyt rahoitusalailla töitä. Bitcoinia Selosmaa (2022) on seurannut kymmenen vuotta ja ottanut sitä myös osakeyhtiönsä taseeseen.
Henri Väkeväinen (2022)	Väkeväinen (2022) on Suomen kryptovaluuttayhdistys Konsensus ry:n hallituksen jäsen. Väkeväisen (2022) koulutustausta on rahoituksen maisteri ja laskentatoimen kandidaatti. Hän on lukenut oikeustieteitä ja ollut pankkialalla töissä. Kaupallisella alalla Väkeväinen (2022) kertoi tehneensä kirjanpitoa ja oikeudellista neuvontaa ja hän mainitsi myös, että hän toimii mukana virtuaalivaluuttojen lainsäädännön puolella.
Martin Wichmann (2022)	Wichmannin (2022) kryptovaluuttatausta alkoi saksalaisen startupin, maksupäätejärjestelmä Blockpayn kanssa. Blockpay integroi vuonna 2016 kryptomaksamisen kivijalkakauppojen POS-päätteisiin, mutta se ei kuulemma ottanut tuulta purjeisiin. Sitä kautta Wichmann (2022) aktivoitui Suomessa paikallisessa kryptovaluuttayhteisössä ja hän oli perustamassa Telegram-ryhmän, jossa on ”tuhatkunta” ihmistä parhaimmillaan. Sitä kautta Wichmann (2022) tutustui Stani Kulechoviin jonka kanssa oli käynnistämässä Aave-nimistä DeFi-alustaa. Tämän jälkeen Wichmann (2022) palasi Suomeen ja perusti yrityksen, joka ei ole kryptovaluuttojen kanssa tekemisissä. Ohessa hän kertoo kuitenkin istuneensa Suomen kryptovaluuttayhdistys Konsensus ry:n hallituksessa ja on nykyään varapuheenjohtajana siinä. Lisäksi hän istuu myös Northcrypton hallituksessa neuvonantajana. Omin sanoin Wichmann (2022) sijoittaa kryptoihin ja harrastaa kryptoja.

Taulukko 1: Asiantuntijahaastattelut

### 3.3 Haastatteluaineiston käsittely ja analysointi

Haastatteluiden videoaineiston ja Microsoft Teamsin automaattisesti luodun litteroinnin tallensin välittömästi yksityiseen tallennustilaan. Kun kaikki haastattelut oli suoritettu, loin

uuden Excel-tiedoston, johon teemoittelin kysymykset ja kirjoitin puhtaaksi lyhennettynä haastattelujen vastaukset.

Teemoittelin kysymykset perustuen tutkimuskysymysten aiheisiin. Aiheet olivat kryptovaluuttojen käyttötarkoitukset, maksujen vastaanottaminen, riskit, toimintatavat useamman henkilön pääsyyn yrityksen kryptovaluuttavaroihin, toimintatavat avainhenkilön menehtymisen varalle, kryptovaluuttojen yksityisyys yrityksessä, lainapalvelut sekä louhiminen. Liitteessä 1 on tarkemmin eritelty haastatteluissa käyttämiäni kysymyksiä. Taulukoinnin jälkeen kirjoitin kysymys kerrallaan haastatteluvastaukset puhtaaksi opinnäytetyöhön. Sellaiset kysymykset, jotka kysyin vain yhdeltä tai muutamalta haastateltavalta esimerkiksi sen takia, että kysymys ei suoraan vastannut tutkimuskysymyksiin, olin suoraan karsinut pois työstä. Tulosluku on rakennettu teemoittelun mukaisessa järjestyksessä.

Haastattelut olivat erilaisia ja osassa haastatteluista käytin videotallennetta, osassa pelkääjän automaattisesti luotua litterointia ja osassa molempia erilaisten puhetyylien ja puheen nopeuden takia, jonka takia esimerkiksi automaattisesti luotu litterointi on ollut epäselvää tai on sisältänyt liikaa virheitä. Excel-tiedostoa käytin nopeaan haastatteluvastauksen hakemiseen opinnäytetyön tuloksia kirjoittaessani.

## 4 Tulokset

Tuloksina tässä opinnäytetyössä toimivat seitsemän asiantuntijahaastattelua. Ensimmäisessä alaluvussa käyn läpi haastatteluvastaukset ilman minkäänlaista analysointia tai pohdintaa. Toisessa alaluvussa teen yhteenvedon vastauksista ja esittelen löytämiäni yhtäläisyyksiä ja eroavaisuuksia vastausten välillä. Seuraavassa luvussa tulen vertailemaan haastatteluvastauksia ja niiden analyysiä tietoaaineistoon ja arvioin haastatteluvastausten validiteettia näiden pohjalta.

### 4.1 Haastatteluiden tulokset

Tässä luvussa käyn läpi seitsemän asiantuntijahaastattelua, joiden vastaukset ovat jaoteltu kahdeksaan eri teemaan alalukujen alle. Teemoittelun avulla haastatteluvastaukset ovat helpompi verrata keskenään ilman tarvetta käydä läpi kaikkia haastatteluvastauksia, vaikka tämän luvun lisäksi vastauksissa oli paljon muitakin mielenkiintoisia keskusteluaiheita. Tutkimuskysymysten takia oli kuitenkin myös tärkeä rajata vastauksia vain olennaisimpiin vastauskategorioihin.

#### 4.1.1 Käyttötarkoitukset

Yritys voi hyödyntää eri tavoilla kryptovaluuttoja osana liiketoimintaa. Henri Väkeväinen (2022) vastasi haastattelussa, että se miten yritys voi hyödyntää kryptovaluuttoja riippuu paljon siitä, minkälainen yrityksen liiketoiminta on. Jos summat ovat isoja, täytyy muun muassa huomioida rahanpesulaki ja selvittää varojen alkuperä. Väkeväisen (2022) mukaan sähköisessä maailmassa on hyvin haastavaa ja kallista selvittää jokaisen asiakkaan henkilöllisyys ja tietoturva täytyy myös tällöin olla hyvällä tasolla. Kolmatta osapuolta voi myös käyttää esimerkiksi vastaanotettujen varojen vaihtamiseksi fiat-valuutaksi, niin kuin Väkeväisen (2022) mukaan monet yritykset tuntuvat käyttävän, jolloin maksuja vastaanottavan yrityksen ei tarvitse itse säilyttää vastaanotettuja kryptovaluuttavaroja. Jos yrityksellä on ylimääräistä varallisuutta vapaassa pääomassa, niin voi olla Väkeväisen (2022) mukaan kannattavaa sijoittaa pitkällä aikavälillä esimerkiksi Bitcoinin. Tällöin säilytystä pitää miettiä, eli säilytetäänkö kylmäsäilytyksessä, tietokoneella vai mobiilissa. Näissä tietoturva tulee olennaiseksi osaksi ja googlaaminen on Väkeväisen (2022) mielestä huono vaihtoehto, kun on kyse kryptovaluutoista, koska ensimmäisiä hakutuloksia pystyy manipuloimaan maksamalla mainonnasta.

Janne Piironen (2022) on myös sen kannalla, että esimerkiksi Bitcoin voi toimia arvon säilyttäjänä yrityksissä esimerkiksi ostamalla sitä tasaisesti kuukausittain. Piironen (2022) tuo myös esille mahdollisuuden käyttää kryptovaluuttoja lainan vakuutena Suomessa Coinmotion-palvelussa. Kolmas käyttötarkoitus, minkä Piironen (2022) tuo esille, on myös kryptovaluuttojen käyttäminen maksuvälineenä, sillä tarkennuksella, että kryptovaluuttojen käyttäminen maksuvälineenä päälohkoketjussa ei ole ehkä niin houkuttelevaa, mutta salamaverkossa kustannukset voi hänen mukaansa olla pieniä. Globaalisesti maksuja voi myös saada Piironen (2022) mukaan nopeasti, pienillä kustannuksilla ja turvallisesti. Piironen (2022) tuo kuitenkin esille, että lainsäädännön takia lähettäjälle ei ole niin houkuttelevaa käyttää kryptovaluuttoja maksuvälineenä, koska se on aina verotapahtuma, kun maksaa kryptovaluutoilla, eli tyyppillisesti maksaja joutuu maksamaan myyntivoitosta pääomatulovero, joka on 30-34 % voitosta.

Jenni Selosmaa (2022) kertoo, että hänen tarkoituksensa on ollut vain vaihtaa osa yrityksensä taseessa olevasta euromääräisestä arvosta Bitcoinin. Hänen mukaansa Bitcoinista tulee sopiva vaihdon väline vasta sitten, kun verotus muutetaan sellaiselle tasolle, että sitä on järkevä käyttää maksuvälineenä, viitaten samaan kuin Piironenkin (2022), eli Suomessa kryptovaluutat eivät sovi yksityishenkilöille maksuvälineiksi, koska jokainen maksutapahtuma on katsottu verotuksellisesti omaisuuden luovutukseksi. Sitä odotellessa Selosmaan (2022) mukaan yritys voi hyvin käyttää kryptovaluuttoja arvon säilytykseen ja sijoittamiseen, kunhan otetaan huomioon arvon vaihtelun riskin.

Jusa Harju (2022) vastasi vakaasti, että parasta mitä yritykset voivat tehdä tällä hetkellä, on ottaa suoria kryptovaluuttasiirtoja vastaan maksuvälineenä ja säilyttää vastaanotettuja kryptovaluuttavaroja. Harju (2022) kuitenkin toteaa, että suurin osa yrityksistä todennäköisesti kuitenkin vaihtaa vastaanotettuja varoja fiat-valuutaksi tai muuksi sijoitukseksi. Isommat yritykset voisivat Harjun (2022) mielestä käyttää kryptovaluuttasiirtoja suurten varojen siirtämiseen mieluummin kuin perinteisiä valuuttasiirtoja. Esimerkkinä hän nostaa esille yrityksen, joka ostaisi palveluja 100 000 eurolla. Normaalisti tällainen siirto kestäisi useamman päivän siirtyä varsinkin globaalisti ja kustannuksia tulisi myös, kun taas jos molemmilla olisi tili kryptovaluuttapalvelussa tai varat siirrettäisiin kryptovaluuttalompakosta toiseen, niin siirrossa voi parhaassa tapauksessa kestää sekunteja ja kulut ovat murto-osan.

Harjun (2022) mukaan myös pienemmät yritykset hyötyvät mikromaksujen vastaanottamisessa. Hän spekuloi tilanteen, jossa kuukausimaksujen sijasta uutissivustolla voisi maksaa senteissä pelkästään yksittäisen artikkelin lukemisesta, ja myyjällä olisi myös varaa tehdä näin, jos transaktiosta ei menisikään maksupalvelun tarjoajalle kymmeniä senttejä vaan murto-osan siitä vain kryptovaluutan transaktiokuluissa.

Martin Wichmann (2022) tuo esille lukuisia esimerkkejä globaaleista applikaatioista, joissa ei ole keskitettyä palveluntarjoajaa. Yleisesti ottaen Wichmann (2022) kuitenkin toteaa, että käyttötarkoitukset yritykselle riippuu pitkälti siitä, mitä yritys tekee ja mikä sen liiketoiminta on.

Pessi Peuran (2022) mielestä tyypillisin tapa yrityksillä käyttää kryptovaluuttoja osana yrityksen liiketoimintaa on sijoittaa osa kassavaroista kryptovaluuttoihin ja hakea sieltä tuottoa. Toinen tapa on sitoa pääomaa esimerkiksi vakaavaluuttoihin, jotka seuraavat dollarin kurssia, jolloin ei tarvitse luoda erikseen mitään valuuttatiliä vaan se riittää, että ottaa käyttöön jonkun kryptovaluuttapalvelun tätä varten. Kryptovaluuttamaksujen vastaanotto on myös Peuran (2022) mukaan merkittävä käytötapa globaalilla mittakaavalla, mutta Suomessa sitä rajoittaa esimerkiksi verotukseen liittyvät asiat, eli jokainen maksutapahtuma on verotuksellisesti luovutustapahtuma, niin kuin useat muutkin haastateltavat mainitsivat. Louhintaa harjoittaa myös jonkin verran yrityksiä joko päätoimisesti tai muun liiketoiminnan ohella Suomessa, Peura (2022) muisti vielä mainita.

Ville Runola (2022) toteaa, että yleisin ja selvin tiedossa oleva käyttötarkoitus yrityksillä on sijoitusvarallisuuden hajauttaminen. Kansainväliset maksut ovat myös yksi käyttötarkoitus osakeyhtiön toiminnan mukaan, jolloin valuutanvaihtoa pystyy tekemään paljon kustannustehokkaammin.

#### 4.1.2 Maksujen vastaanottaminen

Selosmaan (2022) mielestä monia toimijoita löytyy avustamaan alkuun pääsemisessä, jos yritys haluaa alkaa vastaanottamaan maksuja kryptovaluutoissa. Hän kuitenkin huomauttaa, että kirjanpito täytyy laittaa sellaiseen malliin, että yritys saa maksun eurosummaisena tilille, koska Suomessa on velvollisuus pitää kirjanpitoa euroissa.

Peura (2022) toistaa myös samaa ajatusta siitä, että pitää olla maksupalveluntarjoaja, joka ottaa vastaan maksut kuluttajalta ja muuntaa maksun euroiksi sekä tilittää eurosumman yrityksen tilille. Runola (2022) on myös sitä mieltä, että tämä on paras vaihtoehto ja että Bitpay saattaa olla käytetyin toimija verkkokauppa maksuissa.

#### 4.1.3 Riskit

Kysyessäni suurimmista riskeistä, jotka asiantuntijat näkevät kryptovaluutoissa osana yritysten liiketoimintaa, tulee Väkeväisellä (2022) ensiksi mieleen vastapuoliriskit, eli sijoittaako varat pörssiin vai käytetäänkö kylmälompakkoa säilytystä varten. Väkeväisen (2022) mielestä päivätreidausta harjoitteleva yritys pitäisi laatia ohjeistus, jonka mukaan pörssiin siirretään ainoastaan se määrä kryptovaluuttoja, joilla treidataan ja tämän jälkeen siirretään varat pörssistä pois, eli isoja määriä varoja ei kannata pitää pörssissä. Väkeväinen (2022) varoittaa, että isotkin pörssit voivat vuotaa asiakastietoja ulos, joka johtaa esimerkiksi tietokalasteluihin. Väkeväisen (2022) mielestä Suomessa on tapana rehvastella yritysmaailmassa raha-asioista viihteellä, joten vinkiksi hän antaa sen, ettei näistä asioista puhuta julkisesti. Kryptovaluuttapalveluiden turvallisuudesta Väkeväinen (2022) toteaa sen, että Suomessa palvelujen tietoturva on hyvällä mallilla, vaikka varallisuus on toki niissä pienempi. Pörssit ovat yleisestikin hänen mielestään turvallisempia kuin aikaisemmin ja hän haluaakin muistuttaa, että nurin menneen FTX-pörssin ongelma oli se, että asiakkaiden varoja siirrettiin ja käytettiin yksinkertaisesti laittomasti. Tällaiset asiat vaativat Väkeväisen (2022) mielestä asiakkailta sen, että asiakkaat myös ymmärtävät varojen saattavan olla vaikeasti pois siirrettävissä pörsseistä silloin, kun niitä halutaan nostaa sieltä pois.

Piironen (2022) mielestä riskit eivät kasva huomattavasti, kun yritys keskittyy ydinliiketoimintaansa ja ottaa lisänä aikomus säilyttää sekä kasvattaa pitkällä aikavälillä kryptovaluuttojen kokoa tai jos yritys vain ottaa yhden maksutavan lisää käyttöönsä. Säilyttämisessä sen sijaan voi olla isompia riskejä Piironen (2022) mielestä, jos kryptovaluuttoja otetaan omaan halluunsa, eikä ole hyvää osaamista siihen. Turvallisessa säilyttämisessä on hänen mielestään yleensäkin ihmisriski, jos organisaation sisällä ei olla täysin varmoja säilyttämisen periaatteista tai jos yksityisavaimet olisivat yrityksen sisällä vain yhden ihmisen hallussa.

Harjun (2022) mielestä isoja riskejä löytyy muun muassa, jos käytetään pienempää tai tuntematonta pörssiä. Hän kehottaa tutkimaan tarkasti pörssin taustoja, jos haluaa käyttää

sellaista ulkoista säilytystä varten, että se on luotettava paikka. Harju (2022) toteaa, että moni hurahtaa suuria passiivisia korkotuottoja tarjoaviin tahoihin ja ihmettelevät jälkikäteen, kun kyseiset tahot paljastuvat huijauksiksi tai niitä palveluja hakkeroidaan, koska he eivät panosta niin hyvin tietoturvaluuteen. Harju (2022) suosittelee mielummin käyttämään kylmäsäilytystä varojen säilyttämiseen.

Wichmann (2022) tuo myös esille esimerkin FTX-pörssistä ja toteaa, että yksi suuri riski on vastapuoliriski. Sijoittamisessa ja kryptovaluuttojen vastaanottamisessa sen sijaan Wichmann (2022) ei näe niin suurta riskiä, paitsi jos on oma lompakko, jonka sattuu kadottamaan. Tämän ennaltaehkäisemiseksi Wichmann (2022) suosittelee Multisig-lompakkoa tai tiukasti reguloitua suomalaista säilytyspalvelua. Isoimpia riskejä Wichmannin (2022) mukaan liittyy lainaamiseen volatiileja omaisuusluokkia vastaan.

Runola (2022) haluaa painottaa yrityksen oman riskistrategian tärkeyttä. Riskit ovat hänen mukaansa pienimpiä silloin, kun vain käyttää tunnettuja vakaita vakaavuuksia. Kryptovaluuttojen vaihtaminen euroiksi heti vastaanottohetkellä suojaa Runolan (2022) mukaan arvovaihtelevuutta vastaan. Runola (2022) haluaa huomauttaa, että kryptovaluutat ovat pieni ja uusi sijoitusluokka, joten ne pitäisi hänen mukaansa myös suhteuttaa siinä mielessä sijoitusportfolion kokoon.

#### 4.1.4 Useamman henkilön pääsy kryptovaluuttalompakkoon

Useamman henkilön pääsy kryptovaluuttalompakkoon on Selosmaan (2022) mielestä lähinnä yrityksen sisäinen sopimustekninen asia esimerkiksi osakassopimukseen määriteltävänä asiana. Normaalista taloudenhallinta on yrityksissä rajattu talousjohtajalle, tai sille henkilölle, joka vastaa kirjanpidosta, taloudesta ja maksuista. Selosmaa (2022) ei näe minkä takia tämän pitäisi poiketa kryptovaluuttojen kohdalla normaalista protokollasta, jossa normaalisti ei anneta kaikille osakkaille pääsyä taloudenhallintaohjelmistoihin ja mahdollisuuteen tehdä maksuja tai käyttää yrityksen varallisuutta.

Selosmaan (2022) mukaan jos avaimia tallennetaan moneen paikkaan, niin käytännössä ne ovat sitten myös useammasta paikasta saatavilla. Yrityksissä, joissa on useampia henkilöitä, joille halutaan antaa pääsy yrityksen kryptovaluuttavaroihin, on Multisig-ratkaisu Selosmaan (2022) mielestä hyvä, kunhan sovitaan kuinka monella ja kenellä on pääsy varoihin, tarvitaanko useamman allekirjoitus transaktioihin sekä onko jokin alaraja, jonka ylittyessä tarvitaan useamman henkilön allekirjoitukset.

Harju (2022) ehdottaa, että jokaisella avainhenkilöllä kannattaisi olla kahdennettu kylmälompakko samoihin omistuksiin, mutta kukaan avainhenkilöistä ei tulisi kertoa, missä jokainen säilyttää esimerkiksi avainlukulistan. Teknisesti ottaen hän mainitsee, että jokaiseen laitelompakkoon, kuten Ledgeriin, pystyy tuomaan saman varmuuskopion palautettua, jolloin

sama lompakko toimii useammassa laitteessa samaan aikaan. Jos varat taas säilytetään kolmannen osapuolen palvelussa, niin samalle tilille voisi antaa pääsyn useammalle henkilölle tarvittaessa. Kyseisissä palveluissa on yleensä kaksivaiheinen tunnistus käytössä, jota Harju (2022) suosittelee käyttämään.

Harju (2022) toteaa, että varmuuskopioinnin kannalta avainsanoja ei tule säilyttää samassa paikassa kylmälompakon kanssa, koska esimerkiksi tulipalon sattuessa sekä kylmälompakko että varmuuskopio menevät molemmat siinä. Harju (2022) muistuttaa, että kylmälompakkoahan tarvitaan silloin, kun siellä olevia varoja hallinnoidaan, kun taas avainlukulista voi olla vaikeassakin paikassa, koska ihanteellisessa tilanteessa sitä ei joudu käyttämään. Harju (2022) muistaa kertoa, että netistä löytyy helposti eri tapoja ja esimerkkejä, kuinka avainlukulistaa voisi turvallisesti säilyttää ja hän toteaa, että paperilla esimerkiksi Shamir's Secret Sharing vaikuttaa hyvältä tavalta varmuuskopioida avainlukulista.

Wichmannin (2022) mukaan ”not your keys, not your coins” on hyvä periaate, mutta käytännössä avainsanojen kirjoittaminen paperille ja paperin säilyttäminen turvallisesti on yksittäisen käyttäjän kannalta katastrofi. Hän ehdottaa ratkaisuksi palvelua, joka Multisigiä hyödyntämällä abstraktoisi yksityisavaimet taustalle, jolloin käyttäjä lataisi ja käyttäisi sovellusta niin kuin mitä tahansa muuta sovellusta. Wichmann (2022) toteaa, että Multisig on ihan hyvä vaihtoehto yrityksille, jotka haluavat hallinnoida omia kryptovaluuttojaan ja avaimiaan, mutta pieni tekninen perehdytys kaikille Multisig-osapuolille alkuun olisi kuitenkin suositeltavaa, jotta ymmärretään Multisigin peruseriaatteet. Wichmann (2022) muistaa kertoa, että kolmannen osapuolen palveluita löytyy, jotka käyttäjän puolesta hallinnoivat Multisigiä.

Erot Multisigin ja shardaamisen välillä on Wichmannin (2022) mukaan siinä, että Multisigissä on useampi osapuoli allekirjoittamassa transaktiota, kun taas shardaaminen jakaa avaimen palasiin, jolloin pitää kasata avain uudestaan, kun haluaa palauttaa sen. Riski on hänen mielestään siinä, jos avaimen jakaa esimerkiksi neljään osaan ja yhden osan kadottaa, niin avainta ei pystykään enää palauttamaan. Tähän auttaa se, että on esimerkiksi neljä osuutta, joista kolme riittää avaimen palauttamiseen. Multisig on Wichmannin (2022) mukaan helpompi siinä mielessä, että kun kolme neljästä osapuolesta pääsee paikalle, niin voidaan suorittaa transaktio.

Myös Peura (2022) suosii Multisigiä ja yksityisavaimen säilyttämiseen tai varmuuskopiointiin kolmas osapuoli on hyvä, eli jos yrityksestä vaikka kahdella henkilöllä on avain ja kolmas avain on pankilla, jota käytetään vain tarvittaessa, eli jos jompikumpi näistä yrityksen kahdesta henkilöstä menettää pääsyn omaan avaimeensa, niin voidaan vielä palauttaa lompakko pankissa olevalla avaimella. Peuran (2022) mielestä kaikista turvallisista tavoista on aina mahdollista saada enemmän turvallisia, eli turvallisuutta voi aina lisätä, mutta silloin pitää myös miettiä käytännöllisyyttä. Kryptovaluutoista innostuneet neuvovat Peuran (2022) mukaan

usein uusia käyttäjiä, jotka ovat uusia kryptovaluuttojen parissa, että kryptovaluuttoja ei sa missään nimessä säilyttää minkään palveluntarjoajan palvelussa, koska se on niin riskialtista, vaan ainoa oikea tapa on säilyttää itse varat. Peura (2022) haluaa korjata tätä käsitystä sen osalta, että kryptovaluuttapalvelun käyttäminen varojen säilyttämiseen voi olla toiminnan alkupuolella huomattavasti turvallisempi vaihtoehto kuin se, että alkaa itse säilyttämään varoja.

”Aika paljon joudun kohtaamaan niitä tilanteita, että ihmiset eivät ole ottaneet huomioon sitä, että ne joskus kuolevat ja perinnönjaossa ihmetellään sitten, miten varoihin päästään käsiksi. Vastaus voi olla aika usein se, että ei mitenkään.” (Peura 2022.)

Myös Runola (2022) puoltaa useamman allekirjoituksen lompakkoa, jossa jokainen allekirjoitusosapuoli pääsee yrityksen varoihin tai omiin hallinnoimiin varoihinsa kiinni. Esimerkkinä Runola (2022) osaa kertoa, että jos osakkaita on vaikka kymmenen, niin voidaan vaatia kolme tai seitsemän allekirjoitusta, että pystytään käyttämään varoja. Perinteiden Multisig-lompakoiden lisäksi on myös olemassa MPC-lompakoita, joissa yksittäinen avain jaetaan useammalle taholle, ja sitten niillä allekirjoituksen shardeilla pystytään allekirjoittamaan transaktioita. Runola (2022) pitää molempia, sekä Multisigiä että MPC-lompakkoa, turvallisena tapana säilyttää yrityksen kryptovaluuttavaroja, vaikka mielipiteitä on monenlaisia, kumpi on turvallisempi.

Fireblocks (2023) on keskitetty yritys, joka pitää yhden shardin avaimista itsellään, mikä tarkoittaa sitä, että he eivät pääse varoihin käsiksi, mutta pystyvät tiettyyn pisteeseen asti autamaan varojen palauttamisessa, jos joku avaimista katoaa. Avainten jakaminen useampaan osuuteen useammalle taholle on Runolan (2022) mielestä tehokas keino varmuuskopioida avaimia, mutta julkisesti ei voisi sitten kertoa, kenellä on näitä avaimien osia.

Väkeväinen (2022) suosittelee myös, että osakassopimukseen merkittäisiin se, kenellä on oikeus käyttää yrityksen kryptovaluuttalompakkoa. Hän näkee myös tärkeänä sen, että varmistetaan siitä, että lompakko toimii myös silloin, kun joku sairastuu tai on pidempään poissa. Väkeväisen (2022) mielestä on tärkeää, että jaetaan roolit ja että säilytykseen löytyy yrityksen sisällä ohjeistusta.

Piironen (2022) painottaa yrityksen IT-kumppanin tärkeyttä, jos yrityksellä on tällainen. Hänen mielestään riskit tulevat olla hajautettu niin, että on mahdollisimman vähän yksittäisiä ”single point of failure” -tekijöitä, eli jos esimerkiksi yksittäinen riski toteutuisi, niin kaikki ei olisi vielä tällöin mennyttä. Piironen (2022) mielestä tärkeitä kysymyksiä ovat muun muassa moneenko osaan yksityisavain on hajautettu, miten se palautetaan ja missä varmuuskopiot pidetään.

#### 4.1.5 Toimintatavat avainhenkilön menehtyessä tai avainten kadotessa

Jos on sen kaltainen tilanne, että ei tiedetä missä henkilö on säilyttänyt yksityisavaimiaan eikä ole pääsyä kylmälompakkoon, on mahdollista, ettei lompakkoa ikinä löydetä tai ei ikinä päästä kryptovaluuttoihin käsiksi kryptovaluuttoja yrityksessä käsittelevän henkilön menehtyessä. Tämä tulisi Piironen (2022) mukaan tiedostaa etukäteen ja tämä on se syy, miksi yrityksessä ei tulisi olla vain yksi yksityisavain. Yhtälö ei ole toimiva, joten kannattaa hajauttaa yksityisavain ja kannattaa olla jokin varmuuskopion palautusmahdollisuus. Euroopan alueella toimii ainakin sellainen palvelu kuin Casa (2023), jonka verkkosivuston ”How It Works” -sivulla on idea avattu hyvin. Yksittäinen yksityisavain on Piironen (2022) mukaan tietoturvariski, mutta tilanne muuttuu, jos on vaikka useampi osakas, jotka hallinnoivat yhdessä yksityisavaimia.

Avainten kadottamisen varalle Casa (2023) toimii myös Piironen (2022) mukaan hyvin. Esimerkiksi jos on kolme avainta, joista kaksi on osakkailla ja yksi palveluntarjoajalla, niin yhden avaimen kadotessa yksi avain palautetaan palveluntarjoajalta ja luotaisiin uudestaan yksityisavaimet. Tämä on Piironen (2022) mukaan vähän kuin lukkojen vaihto. Palvelu täytyy kuitenkin ottaa käyttöön etukäteen, se on turha jälkikäteen miettiä näitä asioita.

Selosmaan (2022) mukaan osakassopimuksissa sovitaan usein menetelmät sen varalle, jos esimerkiksi yksityisavainta säilyttävä henkilö menehtyy. Kylmälompakon yksityisavaimen voi antaa kaikille, kenelle se halutaan antaa, se on nimenomaan siitä kiinni, miten yrityksessä asia halutaan päättää. Mikään ei estä Selosmaan (2022) mielestä yksityisavaimia kaikille osakkaille tai halukkaille, jolloin kuka tahansa voi käyttää niitä vaikka yksi menehtyisi ja turvallisintahan se on tällaisessa tapauksessa, että useammalla on pääsy lompakkoon. Selosmaa (2022) kuitenkin suosittelee, että ainakin osa varoista voisi olla kolmannen osapuolen palveluntarjoajan hallussa tällaisia tilanteita ajatellen. Siinä tapauksessa, että yksityisavain vain katoaa, suosittelee Selosmaa (2022) varojen siirtämistä toiseen lompakkoon ja uusien yksityisavainten luomista.

Toimintatavaksi yhden avainhenkilön menehtyessä Wichmann (2022) suosittelee varojen siirtämistä toiseen lompakkoon, jos pystyy, tai vaihtamaan yksi Multisig-osapuoli toiseen käytettävässä Multisig-lompakko. Multisigiä käytettäessä kannattaa olla Wichmannin (2022) mukaan esimerkiksi 3/5-virhemarginaali, eli riski pienenee ja jos vaikka yksi menehtyisi, niin on vielä neljä ihmistä, joista kolme tarvitaan transaktion allekirjoittamiseen. Myös sen varalle, että kadotettaisiin yksityisavain, suosittelee Wichmann (2022) Multisig-lompakkoa. Multisigillä voi myös hänen mukaansa pienentää riskiä, että joku voisi väkivaltaa uhkaamalla saada avainosapuoli siirtämään yrityksen varoja rikolliselle. Laitelompakko on myös hyvä käyttää, jolloin yksityisavaimia ei tarvitse itsessään käsitellä niin paljon.

Jos henkilö, joka menehtyy, on ainut, jolla on pääsy yrityksen kryptovaluuttalompakkoon, ja kaikki menee sen mukana, niin ei voi muuta kuin hyvästellä varat. Peuran (2022) mukaan ensimmäiseksi kannattaa kuitenkin penkoa kaikki paikat läpi, mistä vaan saa laillisesti menehtyneen jäljiltä penkoa yksityisavainten löytämiseksi. Ratkaisuna toimintatavaksi tämän varalta on kuitenkin Peuran (2022) mielestä Multisig-lompakot tai custody-ratkaisuja tarjoava palveluntarjoaja, eli osapuoli, joka huolehtii kryptovaluuttojen säilyttämisestä asiakkaan puolesta. Runola (2022) kannattaa myös useamman allekirjoituksen lompakoita, joista korvataan allekirjoittajien joukosta menehtynyt henkilö. Hänen mukaansa järjestelyjä täytyy vaan tehdä ennakkoon sen varalta, että ainut allekirjoittaja menehtyy tai allekirjoittajista useampi menehtyisi samaan aikaan.

Väkeväisen (2022) mukaan informointi heti muille osakkaille on välttämätöntä, jos yksityisavain tai -avaimen osa kadotetaan ja on riski, että se päätyisi väärin käsiin. Käytäntö pitää myös olla olemassa sen varalle, jotta muut pääsevät vielä varoihin käsiksi.

Ainoa oikea toimintasuunnitelma sen varalle, että yksityisavain on kadonnut ja on riski, että se voisi päätyä väärin käsiin on Wichmannin (2022), Peuran (2022) ja Runolan (2022) mielestä yksimielisesti se, että varat siirretään välittömästi uuteen lompakkoon ennen kuin joku muu ehtii siirtää varat omaan lompakkoonsa. Peura (2022) suosittelee myös tekemään ensin pieniä siirtoja toiseen lompakkoon varmistaakseen, että ne menevät läpi, ja sen jälkeen vasta lähettääsiin loput varoista. Kryptovaluutoissa on kuitenkin hänen mielestään se hyvä puoli, että niiden siirtäminen paikasta toiseen on ketterää.

#### 4.1.6 Yksityisyys

Yrityksen yksityisyyden suojeleminen kryptovaluuttatransaktioita suorittaessa yhteydessä ja koi hieman asiantuntijoiden mielipiteitä. Väkeväinen (2022) ehdottaa eri osoitteen käyttämistä joka transaktiossa. CoinJoin on myös yksi tekniikka häivyttää varojen alkuperää, mutta Väkeväinen (2022) haluaa huomauttaa, että pankit eivät välttämättä tykkää keinoista häivyttää alkuperää, vaikka toimittaisiinkin täysin laillisin perustein.

Piironen (2022) mukaan se alkaa jo sieltä kryptovaluuttojen hankkimisesta, jos ei haluta muiden tahojen tietävän, paljonko yrityksellä on lompakossaan kryptovaluuttoja. Kryptovaluuttoja täytyisi hankkia sillä tavalla, jolla identiteetti ei paljastuisi julkisuuteen. Ensimmäinen tapa Piironen (2022) mukaan on louhinta, jota yritykset harrastavat myös Suomessa. Silloin he eivät tarvitse luovuttaa tietoja ulkopuolisille. Piironen (2022) ehdottaa myös eri osoitteen käyttämistä jokaisessa transaktiossa, jolloin osoitteita ei pystyttäisi yhdistämään niin helposti yritykseen.

Selosmaa (2022) puoltaa myös eri osoitteiden käyttämistä eri transaktioissa, mutta huomauttaa, että jos varat otetaan vastaan johonkin tiettyyn osoitteeseen, niin ne näkyvät myös

silloin siellä osoitteessa julkisesti. Eli hän suosittelee aina uuden osoitteen luomista, kun vastaanotetaan sekä lähetetään varoja.

Harjun (2022) ehdotus on kierrättää kryptovaluuttavaroja pörssin kautta, jolloin ei siirretä varoja suoraan kylmälompakosta asiakkaan lompakkoon, vaan siirretään pörssin kautta, jolloin ei päästä niin helposti jäljille varojen alkuperästä. Näiden keinojen lisäksi on myös olemassa kryptovaluuttoja, joissa on jo valmiiksi yksityisyys integroituna, kuten XMR, eli Monero.

Wichmannin (2022) mukaan yksityisyyttään suojeleva yritys voi säilyttää varojaan kylmälompakossa ja siirtää kuumaan lompakkoon vain ne varat, joita yritys tarvitsee siirtoon. Lompakoiden välillä voi siirtää varoja, mutta niitä voidaan julkisesti seurata myös lompakoiden välillä. Varoja voi siirtää kylmälompakosta myös pörssiin ja sieltä eteenpäin vastaanottajalle, mutta Wichmann (2022) varoittaa, että pörssi toki näkee, mistä varat ovat tulleet.

Pseudonyymisyys suojaa ja Peuran (2022) mukaan voidaan käyttää ketjutuksia, pörssiä tai Coinmotionin tapaista toimijaa välissä, jolloin lohkoketjussa näkyy vain se, että palvelu on lähettänyt varoja vastaanottajalle, jos yritys siirtää ensin varoja kylmälompakosta palveluun.

Runolan (2022) mukaan kryptografisesti toimivia ratkaisuja ei ole niin montaa. On kuitenkin CoinJoinia ja mikseriä, joilla yksityisyys voidaan saavuttaa. Osa keinoista, joilla halutaan suojella yksityisyyttä, näyttävät kuitenkin ulospäin rahanpesulta, vaikka se olisikin tehty puhtaasti yksityisyystarkoituksessa. Yritys voi myös Runolan (2022) mielestä säilyttää tiettyä summaa keskitetyllä toimijalla, mutta sillä toimijalla on kuitenkin näkyvillä, mistä osoitteesta talletus on tullut ja mihin nostot lähtevät, eli sekään ei ole niin vedenpitävä yksityisyyskeino.

#### 4.1.7 Lainapalvelut

Haastattelut suoritettiin joulukuussa 2022, eli juuri muun muassa keskitettyjen lainapalveluiden Celsiuksen ja BlockFin sekä FTX-kryptovaluuttapörssin mentyä samana vuonna Chapter 11-konkurssimenettelyyn Yhdysvalloissa. Kysymyksen teemana olikin, nämä tuoreet tapahtumat huomioiden, mikä olisi hyvä keino yrityksille jatkossa saada korkoa kryptovaluuttavaroille.

Väkeväisen (2022) mukaan jos palvelu esimerkiksi lupaa päälle 10 prosentin tuoton uusille asiakkaille, niin se on Ponzi-huijaus. Suomessa on tiukat sääntelyt siitä, että asiakkaiden varat pitää olla erillään yhtiön varoista. Väkeväinen (2022) kertoo, että hän olisi ainakin itse hyvin varovainen lainapalveluiden suhteen. Pankkimaailmassa on tuttua, että kun lainaa yhdestä palvelusta varoja, niin niitä lainataan taas jostain muualta. Siellä sääntely on Väkeväisen (2022) mukaan kuitenkin huomattavasti tiukempaa ja siellä on muun muassa talletussuojat. Kryptopuolella ei ole talletussuojia, vaan täytyy selvittää itse, onko varat säilytetty luotettavasti.

Piironen (2022) suosittelee myös yrityksiä tekemään kotiläksyt hyvin. Hän suosittelee yrityksiä miettimään, minkä verran yritykset ovat valmiita ottamaan riskejä. Jos luovuttaa kryptovaluuttoja kolmannelle osapuolelle, niin silloin riski on olemassa, että varat menetetään. Kysymys lähinnä yritysten mietittäväksi on Piironen (2022) mukaan se, miten niitä riskejä hallinnoidaan.

Selosmaan (2022) mukaan yrityksellä on ihan sama vastapuoliriski olemassa, jos yritys haluaa kryptovaluutoilleen korkotuottoa, kuin jos haluaa euroilleen korkotuottoa. Pankki on tällöin se vastapuoli eurojärjestelmässä. Pörssit taas eivät ole säilytysosapuolia, eikä ne ole suunniteltukaan säilyttämistä varten. Vastapuolen tuoma riski pitää arvioida, kuten esimerkiksi vastapuolen konkurssiriski. Sen takia se on Selosmaan (2022) mukaan kryptopuolella haastavampaa, koska toimijoita on paljon. Nykyään niitä on vähän vähemmän, koska ne menevät konkurssiin, jotka eivät toimi oikein. Selosmaa (2022) suosittelee tekemään taustaselvitykset tarkkaan, koska yleensä mitä korkeammat korot ovat, niin sitä enemmän riskiä siellä säilytysyhteisön toiminnassa on. Hajautetut DeFi-palvelut eivät Selosmaan (2022) mielestä sovi yrityksille varojen säilyttämispaijaksi, koska ne vasta rakentavat ja testaavat toimintaansa. Toki yritys voi ottaa riskejä ja käyttää rahoja eri tavalla, jos yritys nimenomaan hakee tuottoa.

DeFi-palveluiden kannalla sen sijaan on ainakin Wichmann (2022), joka ehdottaa yhdeksi vaihtoehtoksi Aave-lainapalvelua, josta saa korkoa sille, että lainaa kryptovaluuttoja likviditeetti-puoleihin. Toisena hyvänä vaihtoehtona hän suosittelee Ethereumin steikkaamista, jonka korko on varmaan 10 prosentin paikkeilla Ethereumin pääverkkoa validoidaessa, eli todellinen tuotto riippuu missä etherin arvo menee. Wichmann (2022) mainitsee, että CeFi-palvelut ovat osasyys viimeisimpään karhumarkkinaan, koska lainamarkkinoilla oli liikaa vipua. Sen sijaan esimerkiksi Aave-lainassa DeFi-puolella ei ole vastapuoliriskiä, eli palvelu likvidoi automaattisesti lainat, jos ei ole tarpeeksi vakuuksia. DeFi-palveluissa riski on rakennettu protokollaan ja se on läpinäkyvä.

”Niihin palveluihin, mitkä ovat vielä tämän karhumarkkinan jälkeen pystyssä, voidaan taas vähän enemmän luottaa. Ne, jotka ovat konkurssissa, niin ovat sitten konkurssissa.” (Wichmann 2022.)

Peura (2022) toteaa, että kuluttajilla on rapissut luottamus lainamarkkinoihin ja alan toimintaedellytykset näyttävät hyvin haastavilta. DeFi-maailmassa sen sijaan on turvallisia tapoja lainata rahaa ja hakea korkotuottoa. Peura (2022) suosittelee myös yleisesti steikkaamista, joka ei perustu lainaamiseen, vaan protokollan ylläpitoon. Steikkauksessa on hänen mielestään paljon tulevaisuutta ja sitä voi myös yritykset tehdä.

Runolan (2022) mukaan keskitettyjä korontarjoajia, jotka läpinäkyvästi tarjoavat korkoa kryptovaluutoille, on tällä hetkellä aika rajallisesti. Isoja ja moneen kertaan auditoituja yleisesti luotettuja DeFi-palveluita ovat Aave ja Compound. Myös Runola (2022) suosittelee Ethereumin

steikkaamista, ja sitä voi hänen mukaansa myös hajautetusti steikata esimerkiksi Rocket Poolin kautta.

#### 4.1.8 Louhiminen

Selosmaan (2022) mukaan liiketoiminnan kannalta kannattaa tehdä laskelmat, jos yritys aloittaa louhinnan. Bitcoinin louhinta perustuu Proof of Workiin, eli se vaatii louhintatehoa sekä sähköä, kun taas Ethereumin uuden päivityksen myötä sen louhinta perustuu omistamiseen, eli steikkaamiseen. Ethereumin louhintaa varten panostetaan siis varoja siihen, että pääsee varmentamaan sen lohkoketjua. Steikkaaminen ei vaadi sähköä, eikä kovin kummoista laitteistoakaan. Se vastaa enemmän sijoittamista, eli panostetaan ether-varoja saadakseen lohkopalkkioita verkosta.

Selosmaan (2022) mielestä nyt ei ole sopiva aika aloittaa mitään PoW-louhintaoperaatiota. Hänen mukaansa niitä menee tällä hetkellä enemmän konkurssiin kuin nousee uusia. Toisaalta Selosmaa (2022) toteaa, että jos on mahdollisuus saada uusiutuvaa energiaa, mikä ei maksa paljon, ja on laitteistoa valmiina, niin on olemassa erilaisia sivustoja, joissa voi laskea oman kaluston ja sähkön hinnan perusteella louhimisen kannattavuuden. Mitä uudempi ja tehokkaampi laitteisto on, niin sen parempi on laskentateho, mutta ne kannattaa kuitenkin laskea.

Harju (2022) toivoo, että tulisimme vielä näkemään louhimisen tuottoisana. Hänen yrityksensä ei ole kuulemma toistaiseksi vielä myynyt alihinnalla laitteistoa pois, vaan he säilyttävät niitä vielä. He uskovat, että louhiminen palaa vielä plusmerkkiseksi, mutta että on vaikea sanoa palaako se ihan yhtä tuottoisaksi kuin ennen. Harjun (2022) mielestä joka ikinen yritys kannattaisi laittaa tietokoneet louhimaan aina silloin, kun niitä ei käytetä, jos yrityksellä on tietokoneita ja käytetyn sähkön osuus rahassa on pienempi kuin louhinnasta saatu tuotto. Tehottomiakin tietokoneita kannattaa hänen mielestään käyttää, jos ne tuottavat ilmaista rahaa. Louhinta ei Harjun (2022) mukaan kuluta näytönohjaimia, koska silloin kun tietokone käyttää näytönohjainta louhimiseen, niin usein näytönohjainta jopa alikellotetaan, jotta saadaan optimi pieni virrankulutus louhintaa varten. Riippuu toki mitä louhitaan ja millä asetuksilla, mutta Harju (2022) kuvailee louhimista näytönohjaimen ekomoodiksi.

Harju (2022) ottaa myös puheeksi louhimisen lämpöhyödyn. Jos tietokoneet pystyvät tuottamaan louhinnan avulla yrityksen tiloihin, vaikka yhden tai kaksi astetta lämpöä lisää, niin perinteiset lämmityskeinot jäävät pienemmälle käytölle. Sekin säästää, koska lämpö tulee tuotavasta toiminnasta, eli se on hukkalämmön hyötykäyttöä. On myös Harjun (2022) mukaan olemassa louhintaohjelmistoja, jotka toimivat Windowsin päällä ja joita voi asettaa louhimaan silloin, kun esimerkiksi hiirtä ei liikuteta muutama minuuttiin, jolloin taustalla käynnistyy louhintaohjelmisto, joka louhii, kunnes hiirtä taas liikutetaan, jolloin louhinta lakkaa. Se ei hänen mukaansa hidastaisi yrityksessä mitään toimintoja.

Peuran (2022) mukaan näytönohjainlouhinta on tavallaan olemassa Ethereumin ansiosta. Vielä on muitakin protokollia, mitä louhitaan näytönohjaimilla, mutta hänen mukaansa selvästi yli 90 prosenttia näytönohjainlouhinnasta keskittyy Ethereumin louhintaan. Bitcoinin louhintalaitteet, joilla haetaan myös lämmityshyötyä, voi Peuran (2022) mukaan olla järkeviä ratkaisuja yrityksille, jos louhitaan aina öisin ja tuulisina päivinä tai yleensäkin silloin, kun sähkön hinta on riittävän matalalla. Jos on tietoteknistä osaamista, niin järjestelmät voidaan virittää niin, että ne ovat automaattisesti päällä, kun sähkön hinta on alle tietyn rajan ja automaattisesti menevät pois päältä, kun sähkön hinta nousee yli tietyn rajan. Peura (2022) uskoo, että kun Suomessa on kylmä ja halutaan lämmittää tiloja, niin louhinnassa voisi olla potentiaalia, jos melu ei haittaa.

Runolan (2022) mukaan aloitus- ja laitekustannukset tuovat kynnyksen louhinnan aloittamiselle. Jos yrityksellä on näytönohjaimia valmiina, niin niitä kustannuksia ei välttämättä ole, mutta lopulta kysymys on siitä, paljonko sähköstä maksetaan. Jos kyseessä ei ole tehdas, jolla on käytännössä runkoverkkoliittymä tai muuten saa jostain todella halpaa sähköä, niin louhinta ei tule olemaan Runolan (2022) mielestä pitkässä juoksussa kannattavaa. Uusien laitteiden hankinta on hänen mielestään järkevää, jos ajatuksena on hyödyntää hukkalämpöä tai jos on pääsy oikeasti halpaan sähköön. Itsessään laitteiden olemassaolo ei tuo hänen mukaansa etua siihen, että suuremmassa mittakaavassa aloitettaisiin louhimaan.

#### 4.2 Tulosten yhteenveto

Asiantuntijoiden mukaan kryptovaluutoilla voi olla neljä selkeää käyttötarkoitusta osana yrityksen liiketoimintaa: sijoittaminen, säilyttäminen, louhiminen sekä maksujen vastaanottaminen. Säilyttämistä harjoittava yritys tulisi huolehtia tietoturvasta riittävällä tasolla. Haastattelussa tuli ilmi, että jos yrityksellä ei ole tarpeeksi hyvää tietoturvaosaamista ja tietoa kryptovaluuttojen turvallisesta säilyttämisestä, niin hyvä vaihtoehto on käyttää kolmannen osapuolen palvelua tähän tarkoitukseen. Suomalaiset Finanssivalvonnan valvomat maksulaitokset, kuten Coinmotion ja Northcrypto, ovat asiantuntijoiden mukaan luotettavia vaihtoehtoja muun muassa sen takia, että asiakkaiden varat säilytetään erillään niitä hallinnoivan yrityksen kirjanpidosta. Tämä tarkoittaa sitä, että esimerkiksi kyseisen palvelun mennessä konkurssiin asiakkaiden varat eivät ole osa konkurssipesää. Haastattelussa kävi myös ilmi, että isommille yritysasiakkaille voidaan tarjota myös sellaisia palveluita, joita ei kuluttaja-asiakkaille tarjota, kuten esimerkiksi OTC-ostoja.

Maksujen vastaanottaminen ei ole kuluttajille niin houkuttelevaa Suomessa lähinnä verotusyistä, eli kuluttajille jokainen myynti on verotapahtuma, joten maksujen vastaanottamiselle kryptovaluutoissa ei löydy tällä hetkellä asiantuntijoiden mielestä Suomessa kysyntää. Yritykselle se ei kuitenkaan ole niin vaikeaa. Osa asiantuntijoista suosittelee kolmatta osapuolta maksurajapinnan tarjoajaksi, joka muuttaa kryptovaluutat euroiksi ja tilittää eurot yrityksen

tilille. Sellainen yritys, joka vastaanottaisi suoraan kryptovaluuttoja, joutuisi ilmoittamaan ne joka tapauksessa euroissa, koska kirjanpito pitää olla suomalaisilla yrityksillä euroissa.

Yritykset, jotka hallinnoivat ja säilyttävät itse kylmälompakoissa yrityksen kryptovaluuttavaroja, joutuvat miettimään tarkkaan säilyttämiseen liittyviä riskejä, kuten tietoturvariskejä. Asiantuntijoiden mukaan yritysten ei kannata säilyttää itse kryptovaluuttoja, jos yrityksen sisällä ei löydy tarpeeksi tietoteknistä osaamista tai jos ei muuten olla täysin varmoja, miten säilytetään turvallisesti kryptovaluuttoja tai jos toimintaperiaatteet eivät ole ennalta suunniteltu loppuun asti. Suurin osa haastatelluista suositteli Multisigin käyttöä yrityksen kryptovaluuttatransaktioissa.

Multisig on tärkeä erityisesti sellaisessa tapauksessa, että yrityksessä on useampi osakas, jolloin tarvitaan esimerkiksi kolme neljästä allekirjoitusta transaktion suorittamiseksi ja alle kolmella allekirjoituksella ei pystytä suorittamaan transaktiota. Tämä hajauttaa varojen menettämisen riskiä ja käytännössä estää melkein kokonaan, että ulkopuolinen pahansuova taho saisi pakottamalla tai muulla keinolla pääsyn yrityksen kylmälompakon varoihin.

Osa asiantuntijoista suositteli kirjaamaan jo osakassopimukseen, kenellä on pääsy yrityksen kylmälompakkoon tai oikeus käyttää kryptovaluuttavaroja. Yleensä yrityksissä on erikseen talousosasto tai taloudesta vastaava henkilö, joka samalla tavalla kuin on pääsy yrityksen eurovaroihin, pitäisi myös olla pääsy yrityksen kryptovaluuttavaroihin.

Yritys voi asiantuntijoiden mielestä ennakoida sellaisia tapauksia, että yksi (tai useampi) avainosapuoli kadottaa avaimen tai avainosapuoli menehtyy. Yrityksellä on hyvä olla jo valmiiksi toimintatavat tällaisia tapahtumia ajatellen. Kunhan yrityksellä on Multisig-lompakko käytössä, niin allekirjoitusosapuolia voi yksinkertaisesti vaihtaa, jos vaan allekirjoittajia on vielä tarpeeksi. Varat voidaan myös siirtää uuteen lompakkoon ja luoda uudestaan allekirjoitusosapuolet.

Mikäli yksityisavain, jolla pääsee suoraan käsiksi yrityksen kylmälompakkoon, katoaa ja on riski olemassa sille, että ulkopuolinen pääsisi näin käsiksi yrityksen varoihin, jää ainoaksi keinoksi yrittää siirtää varat uuteen lompakkoon nopeasti ennen kuin joku muu ehtii siirtää omaan lompakkoon varat. Tällaista tapausta varten on myös hyvä ennakoida esimerkiksi käyttämällä alusta asti Multisig-lompakkoa, jolloin yhden avaimen katoaminen ei aiheuttaisi vielä riskiä lompakon varoihin pääsyyn.

Kysymykseni yrityksen transaktioiden yksityisyyden parantamiseksi sai hieman vaihtelevia kysyviä reaktioita ensin, mutta käytännössä yksi helppo keino piilottaa ulkopuolisilta transaktioiden määrää ja yrityksen kylmälompakon löydettävyyttä on käyttää esimerkiksi kryptovaluuttojen säilytyspalvelua tai pörssiä, jolloin sieltä lähetettäessä varoja ei nähdä niin helposti julkisessa lohkoketjussa mistä lompakosta varat ovat peräisin. Toinen keino on käyttää niin

sanottuja sekoituspalveluita tai CoinJoinia, mutta näiden käyttäminen aiheuttaisi lähinnä viranomaisten selvityspyyntöjä tiukkojen rahanpesusäädösten takia, vaikka toiminnassa ei itsessään olisi mitään laitonta.

Louhiminen sai enimmäkseen kannatusta asiantuntijoilta, mutta suurin osa asiantuntijoista painotti kannattavuuslaskelmien tärkeydestä. On käytännössä kahta eri tapaa louhia, joista toinen, steikkaaminen, muistuttaa lähinnä sijoitustoimintaa. Toisessa perinteikkäämmässä louhimismuodossa, eli Proof-of-Work-louhinnassa (jota esimerkiksi Bitcoinin louhiminen on), käytetään laitteistoa ja sähköä. Asiantuntijoiden mielestä tällä hetkellä ei varsinkaan uusien investointien tekeminen PoW-louhimista varten ole välttämättä kannattavaa, mutta osa oli kuitenkin sitä mieltä, että nykyisten laitteistojen avulla voisi hyvin louhia, jos vaan sähkö on edullista ja yritys on laskenut, että sähkön jälkeen yritys jäisi voiton puolelle. Osa myös oli sitä mieltä, että louhimisella voisi hyvin korvata ainakin osittain muita lämmitysmuotoja, vaikka louhimista ei tekisikään tulostuloksissa, koska jokainen tuottava lämmityskeino on aina parempi kuin sellainen, joka ei tuota.

Kaikilla asiantuntijoilla on tiedossa muun muassa FTX-pörssin konkurssi ja Terra Lunan romahdaminen sekä sitä seurannut Celsius-lainapalvelun konkurssi, joten on ymmärrettävää, että keskittyneitä lainapalveluja haastatteluun vastanneet eivät erityisemmin suosittele. Sen sijaan hajautettuja DeFi-lainapalveluja, kuten Aave-lainapalvelua, osa asiantuntijoista suosittelevat tuottoa kryptovaluutoille tavoitteleville, koska niissä ei ole vastapuoliriskiä, vaan palvelu likvidoi automaattisesti lainat, joissa ei ole tarpeeksi vakuutta. Myös esimerkiksi Ethereumin steikkaaminen sai kannatusta, koska tuotto tulee suoraan Ethereum-verkon validoinnista, eli protokollan ylläpidosta. Edes suomalaisuus ei tuo keskittyneille korkopalveluille erityistä etua, kun juuri loppuvuodesta 2022 tuli julki suomalaisen Tesseractin korkotilin luottotappiot.

## 5 Johtopäätökset ja pohdinta

Seuraavissa alaluvuissa esitän omat johtopäätökseni tietoperustan ja tutkimustulosten pohjalta sekä pohdin ja reflektoin tutkimusta kokonaisuudessaan. Viimeiseksi esitän loppusanat, jatkotutkimusehdotuksen sekä kiitokset.

### 5.1 Johtopäätökset

Tämän opinnäytetyön tavoitteena oli vastata seuraaviin tutkimuskysymyksiin:

- Miten voidaan käsitellä ja säilyttää kryptovaluuttoja turvallisesti osakeyhtiössä, jossa on useampi osakas?
- Mitkä ovat hyviä toimintatapoja kryptovaluuttojen käsittelemiselle, jos usean osakkaan osakeyhtiössä osakas menehtyy tai yksityisavain katoaa?

- Millä tavoin osakeyhtiö voisi ansaita tuottoa kryptovaluuttaomistuksilleen tai hyödyntää louhimista?

Kryptovaluuttojen turvallisen hallinnoinnin onnistuminen yrityksissä riippuu monesta asiasta. Ensinnäkin yrityksen koko ja avainhenkilöiden määrä on merkittävä tekijä. Pienessä yrityksessä, jossa on vain yksi tai muutama osakas, eikä varsinaisesti palkattua henkilökuntaa, on yleensä talousasiat yhden osakkaan varassa tai kaikilla saattaa olla yhtäläinen oikeus käsitellä yrityksen taloutta, pankkitiliä ja muuta varallisuutta. Isommissa yrityksissä on usein talouspäällikkö tai -osasto, joka käsittelee yrityksen taloutta ja kirjanpitoa. Kryptovaluuttavarojen ei pitäisi olla poikkeus; sama henkilö tai osasto, joka käsittelee taloutta, on myös se taho, joka käsittelee mahdollisia kryptovaluuttavaroja.

Pienessä osakeyhtiössä, jossa on esimerkiksi kolme osakasta, voisi olla hyvä ajatus käyttää Multisig- tai MPC-kylmälompakkoa kryptovaluuttavarojen säilyttämiseen. Esimerkkitapauksessa optimaalisin keino on vaatia kaksi allekirjoitusta kolmesta, jolloin yhden avainhenkilön ollessa estynyt riittää, että kaksi allekirjoittajaa on läsnä, halutessaan suorittaa transaktio kylmälompakosta. Toinen tapa säilyttää kryptovaluuttavaroja on säilyttää varat suomalaisessa Finanssivalvonnan hyväksymässä kryptovaluuttapalvelussa, kuten Coinmotionissa tai Northcryptossa. Samassa palvelussa pystytään myös sijoitusmielessä ostamaan automaattisesti kuukausittain kryptovaluuttoja euroja vastaan, eli DCA-strategialla (engl. dollar cost averaging), jolloin säästytään ylimääräisistä siirroista palveluista ulos ja pienennetään riskiä kryptovaluuttavarojen hukkaamiselle. Palveluun voi antaa yhdelle tai useammalle henkilölle käyttäjätunnuksen ja salasanan. Hyvä suositeltu turvakeino on myös käyttää kirjautumisen yhteydessä monivaiheista tunnistautumiskeinoa, jolloin pelkästään käyttäjätunnuksen ja salasanan hukkaaminen ei vielä aiheuta välitöntä vaaraa ulkopuolisille transaktioiden suorittamiseen.

Toimintatavat ovat myös aina tärkeitä kirjata ylös etukäteen yrityksissä muun muassa sen varalta, että kryptovaluuttavaroja käsittelevä henkilö menehtyisi tai hukkaisi yksityisavaimen. Kryptovaluuttapalveluissa tällainen tapahtuma ei luo vielä suurta vahinkoa yrityksen varoille, jos vaan muilla henkilöillä yrityksessä on vielä pääsy kyseiseen palveluun. Sen sijaan itse hallinnoimissa kylmälompakoissa riski varojen menettämiselle on todellinen, jos ei olla ennakoitu tällaista tapahtumaa etukäteen ottamalla esimerkiksi Multisig käyttöön tai jos vain yhdellä henkilöllä on pääsy kylmälompakkoon ja kyseisen lompakon yksityisavainta ei löydy. Koska yksityisavain on turvallisesti kryptografisesti salattu, voi varojen palauttaminen olla mahdollista. Keskitetyissä palveluissa on yleensä mahdollista, niin kuin pankeissakin, antaa pääsy toiselle henkilölle yrityksen varoihin, mutta tällöin on tärkeä muistaa, että vastapuoliriski on todellinen silloin, kun kryptovaluuttavarat eivät ole omassa hallussaan.

Vastapuoliriski on myös todellinen, ellei jopa erittäin todennäköinen silloin, kun käyttää tuotteiden tavoittelemiseen kryptovaluuttavaroille keskitettyä lainapalvelua. Yhdysvaltalaiset

keskitetyt lainapalvelut Celsius ja BlockFi hakeutuivat Chapter 11 -konkurssimenettelyyn vuonna 2022 asiakkaiden todennäköisesti menettäessään lopullisesti niihin palveluihin sijoittamansa kryptovaluuttavaransa. Mikään muukaan keskitetty lainapalvelu ei edes ideana ole hyvä keino saada tuottoa kryptovaluuttavaroille, varsinkaan yrityksille. Sen sijaan tuottoa tavoitteleva sijoittaja voisi käyttää korkotuoton tavoittelua varten hajautettua DeFi-lainapalvelua, kuten Aave-palvelua, tai sitten esimerkiksi Ethereum-steikkaamista, joka on periaatteessa sijoittamista muistuttavaa louhintaa. Hajautettujen lainapalveluiden tuotto on sisäänrakennettu protokollaan tehden siitä luotettavan sijoituskeinon. Steikkaaminen on verkon validoimiskeino, jolla voi saada kryptovaluutassa tasaista tuottoa, mutta arvo fiat-valuutassa riippuu täysin kurssiin, jos steikkaustuottoa ei haluta välittömästi myydä esimerkiksi euroja tai vakaavaluutaa vastaan.

Toimitilaa hallinnoivalla yrityksellä voisi olla intressissään käyttää louhintalaitteiden tuottamaa lämpöä hyödyksi tavoitellen samalla louhintatuottoa. Tämä edellyttää jonkin verran tietoa ja taitoa louhinnasta, mutta tekemällä laskelmat tarkkaan yritys voisi ainakin säästää lämmityskustannuksissa. Louhintaa miettiessä yrityksen pitäisi ottaa huomioon muun muassa sähkön hinta sekä onko mahdollista ohjelmoida louhintalaitteet louhimaan vain silloin, kun pörssisähkö on tarpeeksi edullista. Louhintaa varten täytyisi myös löytyä soveltuvat laitteet; pelkkä toimistotietokone ei välttämättä riitä, vaan nykyään koneesta täytyisi löytyä suhteellisen uusi ja tehokas näytönohjain tai sitten louhintaa varten pitäisi hankkia pelkästään louhintaan soveltuvia ASIC-laitteita. Tällä hetkellä uusien louhintalaitteiden tai näytönohjainten hankkiminen louhintaa varten ei ole kustannustehokasta, mutta tilanne voi muuttua tulevaisuudessa. Yrityksen kannattaa siis seurata markkinoita, jos louhintatuotto ja hukkalämmön hyödyntäminen kiinnostaa.

Jos yrityksellä on intressissään vastaanottaa maksuja kryptovaluutoissa, niin yrityksen kannattaa ottaa huomioon verotukselliset ja kirjanpidolliset näkökulmat. Jos yritys ei muuten säilytä kryptovaluuttoja, niin kryptovaluuttamaksujen vastaanottaminen suoraan voi olla aikaa vievää ja verotuksellisesti tehotonta. Kirjanpidossa jokainen kryptovaluuttamaksun vastaanotto täytyy ilmoittaa euroissa, joten tällaisessa tapauksessa kolmannen osapuolen palvelu, joka vastaanottaa kryptovaluuttamaksun ja vaihtaa maksun euroiksi ennen tilitystä, voisi olla hyvä ja järkevä vaihtoehto. Jos yritys ei muuten ole kryptovaluuttojen kanssa tekemisissä, niin olisi hyvä saada äsken mainitut ylimääräiset vaiheet pois kaupanteosta ja käyttää suosiolla kolmannen osapuolen palvelua maksujen vastaanottamisessa.

## 5.2 Omaa pohdintaa opinnäytetyöstä ja tutkimuksesta

Seuraavaksi pohdin opinnäytetyön luotettavuutta sekä avoimuutta ja tietosuoja. Tämän jälkeen pohdin työni eettisiä kysymyksiä sekä opinnäytetyön hyödyllisyyttä ja käyttökelpoisuutta.

### 5.2.1 Opinnäytetyön luotettavuus

Olen käyttänyt opinnäytetyöni lähteinä alan ajankohtaista tietokirjallisuutta sekä avoimen lähdekoodin teknologiaa kuvailevia kirjoituksia. Kyseiset avoimiin lähdekoodeihin perustuvat kirjoitukset ovat helppo todentaa luotettaviksi, koska paikkansa pitämättömät kirjoitukset voidaan helposti kumota sellaisten toimesta, jotka ymmärtävät lähdekoodia. Esimerkiksi koko Bitcoinin koodi löytyy verkosta. Jos joku taho väittäisi, että Bitcoinissa on sellainen ominaisuus, mitä siinä ei todellisuudessa ole, niin useat ihmiset kiinnittäisivät tällaiseen välittömästi huomionsa ja ne verkkosivustot, joissa tällaiset kirjoitukset ovat olleet esillä, menettäisivät arvonsa. Sosiaalisessa mediassa myös menettävät suosionsa sellaiset julkaisut, joissa ei olla linkitetty luotettaviin verkkosivustoihin. Alan harrastajat osaavat erottaa luotettavat blogi- ja uutissivustot.

Opinnäytetyössäni olen kuvaillut kryptovaluuttojen turvallisuutta eri käyttötarkoituksissa käyttäen alan asiantuntijoiden kirjoituksia, tietokirjallisuutta sekä haastatteluja. Tämän perusteella alan harrastaja pystyy todentamaan helposti, jos jokin asia ei pidä paikkansa tässä työssä.

Bitcoin ja monet muut kryptovaluutat ovat avoimen lähdekoodin teknologioita, joista ei ole löydetty merkittäviä aukkoja vuosien varrella, joten teknologiasta itsestään en ole tarvinnut etsiä paljon vertaisarvioituja tutkimuksia. Totta puhuen, suurin osa kryptovaluutoista ja toke-neista ovat kuitenkin roskaa. Luotettavien kryptovaluuttojen tunnistamiseksi ei tarvita muuta kuin CoinMarketCapin (2023a) etusivun tutkimista, josta selviää kryptovaluutan markkina-arvo ja volyyymi pörseissä sekä muun muassa fiat-arvo, tarjonta ja taustatiedot.

### 5.2.2 Opinnäytetyön avoimuus ja tietosuoja

Opinnäytetyö on suoritettu avoimesti, lukuun ottamatta toimeksiantajan yksityisyyden suojaamista sekä asiantuntijoiden haastatteluvastauksia kokonaisuudessaan. Asiantuntijahaastattelut ja tietty sähköpostiviesti ovat myös ainoat lähteet, jotka ovat julkaisemattomia lähteitä. Asiantuntijoiden haastattelut suoritettiin Microsoft Teams -alustalla ja haastattelut nauhoitettiin videomuotoon sekä litteroitiin automaattisesti Teams-ohjelmassa. Haastatelluille kerroin etukäteen, että haastattelu nauhoitetaan omien muistiinpanojeni helpottamiseksi. Lupasin myös poistaa nauhoitukset sen jälkeen, kun opinnäytetyö on valmis ja julkaistu, koska ei ole tarvetta säilyttää nauhoituksia enää sen jälkeen.

Kaikki tietoaineisto, haastattelunauhoitukset sekä toimeksiantajan dokumentit on säilytetty henkilökohtaisella pilvipalvelutililläni. Pilvipalvelutilini on salasanasuojattu monivaiheisella tunnistautumisella ja tietokoneeni ovat myös salasanasuojattu. Toimeksiantajan nimi ja yhteyshenkilö on Laurea-ammattikorkeakoulun PRM-järjestelmässä mainittu, muuten toimeksiantajan tahtoa tulla mainitsematta opinnäytetyössä on kunnioitettu.

### 5.2.3 Eettiset kysymykset

Opinnäytetyössä ei ole tarkoitus jakaa sijoitusneuvoja. Eettisyys on huomioitu siltä osin rajamalla opinnäytetyö vain informatiiviseksi työksi tai oppaaksi toimeksiantajalle sekä muille yrityksille, jotka käsittelevät tai tulevat tulevaisuudessa käsittelemään kryptovaluuttoja osana yrityksen liiketoimintaa. Opinnäytetyössä ei suositella tiettyjä kryptovaluuttoja niiden arvon perusteella, vaan tiettyjä kryptovaluuttoja tai konsensusmekanismeja luetellaan ominaisuuksineen lähinnä teknisestä näkökulmasta.

DeFi-palveluita ja steikkausta on myös suositeltu tuottoa tavoitteleville sijoitusosapuolille protokollan takia, joka poistaa vastapuoliriskin. On kuitenkin selkeästi kerrottu, että suositus perustuu protokollaan tuottamaan passiiviseen tuloon, eikä kryptovaluutan arvonnousuun.

En tunne yksityiselämässäni enkä ole sukua haastateltuihin tai muihin opinnäytetyössä mainittuihin lähteisiin. En ole myöskään taloudellisesti kytköksissä mihinkään tietoaaineistossa, haastatteluissa tai lähteissä mainittuihin yrityksiin. Poikkeuksena haluan kuitenkin mainita avoimuuden kannalta Coinmotionin, josta omistan 20 kpl osaketta, jotka olivat arvoltaan ostohetkellä yhteensä 1540 euroa. Tämä on mielestäni merkityksetön määrä osakkeita, enkä tule saamaan taloudellista tai muuta hyötyä mainitsemalla Coinmotionia opinnäytetyössäni.

### 5.2.4 Tutkimuksen hyödyllisyys ja käyttökelpoisuus sekä tutkimuksen aikataulu

Opinnäytetyösuunnitelman alkuperäisen aikataulun mukaan opinnäytetyön piti valmistua marraskuussa 2022. Juuri ennen haastattelupyyntöjen lähettämistä tapahtui kryptovaluuttojen historian yksi suurimmista mustan joutsenen tapahtumista, nimittäin FTX-pörssin kaatuminen. Kyseinen tapahtuma vaikuttaa merkittävästi muun muassa siihen, miten luotettavina kolmannen osapuolen keskitetyt pörssi-, välitys- ja säilytyspalvelut voidaan nähdä. Tein tämän takia harkitun päätöksen siirtää haastatteluja myöhempään ajankohtaan joulukuun 2022 puolelle ja tammikuussa 2023 kävin haastatteluaineistoa läpi.

Uskon, että sain enemmän hyödyllistä ja ajantasaista tietoa opinnäytetyöhön joustavalla aikataulutamisella. Jos opinnäytetyö olisi valmistunut vuoden 2022 syksyllä, olisi osa opinnäytetyön tiedosta ollut vanhentunutta jo vuoden 2023 alussa. Kryptovaluuttojen historia on lyhyt ja pienetkin tapahtumat voivat muuttaa merkittävästikin alan tulevaisuutta.

## 5.3 Tulosten raportointi toimeksiantajalle

Opinnäytetyön valmistuttua tulen olemaan toimeksiantajaan yhteydessä. Toimeksiantajan halutessa olen valmis esittelemään työni ja keskustelemaan tuloksista.

Toimeksiantajan tulee tehdä omat päätökset jatkotoimenpiteitä varten, enkä ole vastuussa opinnäytetyön kirjoittajana yrityksen tekemistä strategisista tai taloudellisista päätöksistä, jotka pohjautuvat opinnäytetyössä esiteltyihin neuvoihin.

#### 5.4 Loppusanat, jatkotutkimusehdotus ja kiitokset

Opinnäytetyö oli oppimiseni kannalta tärkeää ja mielenkiintoista. Opinnäytetyön tekemiseen kului paljon aikaa ottaen huomioon rajallinen vapaa-aikani ollessani kokopäivätyössä. Kryptovaluutat itsessään ovat kuitenkin mielestäni mielenkiintoinen ja uusi aihe enkä kadu aihevalintaani. Suosittelen kaikkia tämän työn lukijoita perehtymään kryptovaluuttoihin ja tutustumaan niiden tuomiin mahdollisuuksiin. Sijoittamista harkitsevia neuvon kuitenkin tekemään aina omat taustatutkimukset eikä pelkästään luottamaan minun tai kenenkään muunkaan sanoihin. Sijoituksiin, niin kryptovaluuttoihin kuin muihinkin sijoitusluokkiin, kannattaa laittaa kiinni vain se raha, jota on varaa hävitä. Tämä koskee myös yrityksiä.

Jatkotutkimuksena ehdottaisin selvitystä pankkien ja rahoituslaitosten suhtautumiseen kryptovaluuttoihin osana yrityksen tai yksityishenkilön rahaliikennettä. Pankit voivat yksimielisesti sulkea yrityksiä tai henkilöasiakkaita pankkipalvelujen piiristä ulos pelkästään sen perusteella, että henkilö on tallettanut rahaa pankkitililtään kryptovaluuttapalveluun, vaikka toiminta olisi muuten täysin laillista. Teoria tälle löytyy siitä, että kryptovaluutat eivät ole minäkään keskuspankin liikkeelle laskemia, joten luonnollisesti myös pankit eivät halua asiakkaidensa siirtyvän pankkipalvelujen piiristä pois avoimen ja hajautetun rahapolitiikan piiriin.

Kiitän opinnäytetyön onnistumisesta haastateltuja asiantuntijoita, Suomen kryptovaluuttayhteisöä, ystäviäni, Laurea-ammattikorkeakoulua, perhettäni sekä Satoshi Nakamotoa.

## Lähteet

### Painetut

Ammous, S. 2019. Bitcoin-standardi. Suomentaja Laamanen, N., Oinonen, L., Brand, T., Laitila, T. & Kalergis, A. Helsinki: Oy Nord Print Ab.

ISO 27000 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. 2. painos. Helsinki: Suomen Standardisoimisliitto SFS ry.

ISO 31000 2018. Riskienhallinta. 2. painos. Helsinki: Suomen Standardisoimisliitto SFS ry.

Karame, G. & Androulaki, E. 2016. Bitcoin and Blockchain Security. Norwood, MA, Yhdysvallat: Artech House.

Moilanen, T., Ojasalo, K. & Ritalahti, J. 2015. Kehittämistyön menetelmät - Uudenlaista osaamista liiketoimintaan. 3.-4. painos. Helsinki: Sanoma Pro.

### Sähköiset

Abaday, A. 2021. Blockchain Consensus Protocols | PoW & PoS. Coinmotion. Viitattu 3.2.2023. <https://coinmotion.com/a-short-guide-to-blockchain-consensus-protocols/>

Alexandria 2023. Ticker Symbol. Viitattu 13.2.2023. <https://coinmarketcap.com/alexandria/glossary/ticker-symbol>

Allen, C. & Friedenbach, M. 2019. A New Approach to Social Key Recovery. Viitattu 11.10.2022. <https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/topics-and-advance-readings/social-key-recovery.md>

Banton, C. 2022. How Escrow Protects Parties in Financial Transactions. Investopedia. Viitattu 14.10.2022. <https://www.investopedia.com/terms/e/escrow.asp>

Bédune, J-B. & Guillemet C. 2021. On the security model of software wallets. Ledger Labs. Viitattu 14.2.2023. <https://blog.ledger.com/software-wallets/>

Behnke, R. 2022a. What Is a BIP39? Halborn. Viitattu 3.2.2023. <https://halborn.com/what-is-a-bip39/>

Behnke, R. 2022b. What Is an MPC Wallet? Halborn. Viitattu 3.2.2023. <https://halborn.com/what-is-an-mpc-wallet/>

Binance 2018. How to Complete Entity Verification? A Step-by-Step Guide. Viitattu 12.10.2022. <https://www.binance.com/en/support/faq/360015552032>

BIP-39 2013. Mnemonic code for generating deterministic keys. Viitattu 30.9.2022. <https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki>

Bitcoinkeskus.com 2022. Suomalaiset kauppapaikat ovat turvallisia vaihtoehtoja. Viitattu 13.10.2022. <https://bitcoinkeskus.com/suomalaiset-kauppapaikat-turvallisuus/>

Blockplate 2022. First 4 Letters of a BIP39 Mnemonic Recovery Seed Phrase. Viitattu 12.10.2022. <https://www.blockplate.com/pages/first-4-letters-of-a-bip39-mnemonic-seed-phrase>

Brade, H. 2020. Prasos Oy täytti kahdeksan vuotta. Bittiraha.fi. Viitattu 10.10.2022. <https://bittiraha.fi/blog/prasos-oy-taytti-kahdeksan-vuotta/>

Bradley, E. 2019. Crypto OTC Trading, Explained. Cointelegraph. Viitattu 13.2.2023. <https://cointelegraph.com/explained/crypto-otc-trading-explained>

Buterin, V. 2022. Twitter 9.8.2022. Viitattu 1.10.2022. <https://twitter.com/VitalikButerin/status/1556925602233569280>

Casa 2023. How It Works. Viitattu 3.2.2023. <https://keys.casa/how-it-works/>

Chen, J. 2022a. Fiat Money: What It Is, How It Works, Example, Pros & Cons. Investopedia. Viitattu 14.10.2022. <https://www.investopedia.com/terms/f/fiatmoney.asp>

Chen, J. 2022b. Know Your Client (KYC): What It Means, Compliance Requirements. Investopedia. Viitattu 14.10.2022. <https://www.investopedia.com/terms/k/knownyourclient.asp>

Chohan, U. 2021. A History of Dogecoin. Viitattu 3.2.2023. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3091219](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091219)

CoinMarketCap 2023a. Today's Cryptocurrency Prices by Market Cap. Viitattu 14.9.2022. <https://coinmarketcap.com/>

CoinMarketCap 2023b. Top Cryptocurrency Spot Exchanges. Viitattu 13.2.2023. <https://coinmarketcap.com/rankings/exchanges/>

Coinmotion 2021. Sijoittaminen kryptovaluuttoihin yrityksenä - verotus, kirjanpito ja sijoitusten hallinta. Webinaari. Viitattu 12.9.2022. [https://www.youtube.com/watch?v=47jrIzD\\_nQ](https://www.youtube.com/watch?v=47jrIzD_nQ)

Costea, V. 2019. Bitcoin Wallet Reviews: What's The Best Hardware Wallet on The Market? Part 2. Bitcoin Magazine. Viitattu 3.2.2023. <https://bitcoinmagazine.com/culture/bitcoin-wallet-reviews-whats-the-best-hardware-wallet-on-the-market-part-2>

Cryptonews 2023. How To Make A Bitcoin Paper Wallet? Viitattu 13.2.2023. <https://cryptonews.com/guides/how-to-make-a-paper-bitcoin-wallet.htm>

Deer, M. 2022. Centralized vs. decentralized digital networks: Key differences. Viitattu 17.10.2022. <https://cointelegraph.com/explained/centralized-vs-decentralized-digital-networks-key-differences>

Elinkeinoelämän keskusliitto 2022. Yritysturvallisuus. Viitattu 2.10.2022. <https://ek.fi/hyoty-tietoa-yrityksille/yritysturvallisuus/>

Elliptic Connect 2022. Tornado Cash Mixer Sanctioned After Laundering Over \$1.5 Billion. 8.8.2022. Viitattu 1.10.2022. <https://hub.elliptic.co/analysis/tornado-cash-mixer-sanctioned-after-laundering-over-1-5-billion/>

Ethereum 2022. What is Ethereum? Viitattu 14.9.2022. <https://ethereum.org/en/what-is-ethereum/>

Ethereum Improvement Proposals 2022. Viitattu 17.10.2022. <https://eips.ethereum.org/>

Exodus 2023a. Exodus Bitcoin & Crypto Wallet. Viitattu 14.2.2023. <https://www.exodus.com/>

Exodus 2023b. Exodus + Trezor Hardware Wallet Experience. Viitattu 14.2.2023. <https://www.exodus.com/trezor-wallet/>

Fernando, J. 2022. Inflation: What It Is, How It Can Be Controlled, and Extreme Examples. Investopedia. Viitattu 14.10.2022. <https://www.investopedia.com/terms/i/inflation.asp>

Finanssivalvonta 2019. Finanssivalvonta myönsi viidelle virtuaalivaluutan tarjoajalle rekisteröinnin - valvonnan tavoitteen on rahanpesun estäminen. Viitattu 10.10.2022. <https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2019/finanssivalvonta-myonsi-viidelle-virtuaalivaluutan-tarjoajalle-rekisteroinnin--valvonnan-tavoitteena-on-rahampesun-estaminen2/>

Fireblocks 2023. MPC Wallet As a Service. Viitattu 3.2.2023. <https://www.fireblocks.com/platforms/mpc-wallet/>

Frankenfield, J. 2022. What Does Proof-of-Stake (PoS) Mean in Crypto? Investopedia. Viitattu 2.10.2022. <https://www.investopedia.com/terms/p/proof-stake-pos.asp>

Gnosis Safe 2023. What is Gnosis Safe? Viitattu 3.2.2023. <https://help.gnosis-safe.io/en/articles/3876456-what-is-gnosis-safe>

Hayes, A. 2022. Stablecoins: Definition, How They Work, and Types. Investopedia. Viitattu 3.2.2023. <https://www.investopedia.com/terms/s/stablecoin.asp>

Hyytiäinen, T. 2018. Merkle-puu. Viitattu 17.10.2022. <https://medium.com/lohko-ketju/merkle-puu-5d039617381f>

Investopedia 2022. Deflation: Definition, Causes, Changing Views on Its Impact. Viitattu 14.10.2022. <https://www.investopedia.com/terms/d/deflation.asp>

Katakri 2020. Viitattu 11.10.2022. [https://um.fi/documents/35732/0/Katakri+-+2020\\_1218.pdf](https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf)

Katte, S. 2022. ETHW Core to push on with Ethereum PoW fork 24 hours after Merge. Cointelegraph. Viitattu 3.2.2023. <https://cointelegraph.com/news/ethw-core-to-push-on-with-ethereum-pow-fork-24-hours-after-merge>

KHO 42/2019. Viitattu 13.10.2022. <https://www.kho.fi/fi/index/paatokset/vuosikirjapaatokset/1553685714978.html>

Krayon Digital 2023. MPC Wallet Explained. Viitattu 13.2.2023. <https://www.krayondigital.com/mpc-wallet-explained>

Kyberturvallisuuskeskus 2022. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Viitattu 14.2.2023. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-op-paat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi>

Laki elinkeinotulon verottamisesta 360/1968. Viitattu 13.10.2022. <https://www.finlex.fi/fi/laki/ajantasa/1968/19680360>

Laki virtuaalivaluutan tarjoajista 572/2019. Viitattu 13.10.2022. <https://www.finlex.fi/fi/laki/alkup/2019/20190572>

Ledger 2023a. Compare Ledger hardware wallets. Viitattu 14.2.2023. <https://shop.ledger.com/pages/hardware-wallets-comparison>

Ledger 2023b. Ledger Live. Viitattu 14.2.2023. <https://www.ledger.com/ledger-live>

LocalBitcoins 2019. AML regulation and new features update. Viitattu 3.2.2023. <https://localbitcoins.com/blog/aml-features-update/>

LocalBitcoins 2020. Viitattu 10.10.2022. <https://localbitcoins.com/about>

LocalBitcoins 2023. LocalBitcoins will discontinue its service. Viitattu 13.2.2023. [https://localbitcoins.com/service\\_closure/](https://localbitcoins.com/service_closure/)

Min, A. 2021. A Practical Guide to Bitcoin Addresses. Bitcoin Briefly. Viitattu 3.2.2023. <https://bitcoinbriefly.com/practical-guide-bitcoin-addresses-explained/#address-prefixes-1-legacy-3-nested-segwit-bc1-native-segwit-and-how-to-save-money-on-your-bitcoin-transaction-fees>

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Viitattu 12.9.2022. <https://bitcoin.org/bitcoin.pdf>

Nakov, S. 2018. Practical Cryptography for Developers. Viitattu 17.10.2022. <https://crypto-book.nakov.com/>

Nelson, J. 2022. What Are Coin Mixers and How Do They Work? Decrypt 12.8.2022. Viitattu 1.10.2022. <https://decrypt.co/resources/what-are-coin-mixers-tornado-cash-how-do-they-work>

Northcrypto 2020. Viitattu 10.10.2022. <https://www.northcrypto.com/fi/about>

Open Source Initiative 2007. The Open Source Definition. Viitattu 17.10.2022. <https://opensource.org/docs/osd>

Opendime 2022. Viitattu 27.9.2022. <https://opendime.com/>

Pietarinen, J. 2015. Etiikka. Viitattu 17.10.2022. <https://filosofia.fi/fi/ensyklopedia/etiikka>

Poliisi 2023. Poliisi ei aloita esitutkintaa rahoituslaitoksen toiminnasta. Viitattu 13.2.2023. <https://poliisi.fi/-/poliisi-ei-aloita-esitutkintaa-rahoituslaitoksen-toiminnasta>

Rashid, S. 2018. Multi-signature hardware wallets with Electrum. Viitattu 12.10.2022. <https://saleemrashid.com/2018/01/27/hardware-wallet-electrum-multisig/>

Rusnak, P., Kozlik, A., Vejpustek, O., Susanka, T., Palatinus, M. & Hoenicke, J. 2017. Shamir's Secret-Sharing for Mnemonic Codes. Viitattu 11.10.2022. <https://github.com/satoshilabs/slips/blob/master/slip-0039.md>

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Teemahaastattelu. KvaliMOTV. Viitattu 14.10.2022. [https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6\\_3\\_2.html](https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_2.html)

SatoshiLabs 2021. Multisig and split backups: two ways to keep your bitcoin more secure. Viitattu 12.10.2022. <https://blog.trezor.io/multisig-and-split-backups-two-ways-to-make-your-bitcoin-more-secure-7174ba78ce45>

Singh, J. 2021. Can Bitcoin's hard cap of 21 million be changed? Cointelegraph. Viitattu 13.2.2023. <https://cointelegraph.com/explained/can-bitcoins-hard-cap-of-21-million-be-changed>

Trezor 2022. Shamir Backup. Viitattu 11.10.2022. <https://trezor.io/shamir/>

Trezor 2023. Compare Trezors. Viitattu 14.2.2023. <https://trezor.io/compare>

Tuloverolaki 1535/1992. Viitattu 2.10.2022. <https://www.finlex.fi/fi/laki/ajan-tasa/1992/19921535>

Unchained Capital 2023. Bitcoin multisig vaults. Viitattu 3.2.2023. <https://unchained.com/vaults/>

United States Courts 2023. Chapter 11 - Bankruptcy Basics. Viitattu 13.2.2023. <https://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/chapter-11-bankruptcy-basics>

Wagner, L. 2022. What Is SHA-256? Boot.dev. Viitattu 13.2.2023. <https://blog.boot.dev/cryptography/how-sha-2-works-step-by-step-sha-256/>

Wiktionary 2022. Niukkuus. Viitattu 17.10.2022. <https://fi.wiktionary.org/wiki/niukkuus>

YCharts 2023. Bitcoin Blockchain Size. Viitattu 14.2.2023. [https://ycharts.com/indicators/bitcoin\\_blockchain\\_size](https://ycharts.com/indicators/bitcoin_blockchain_size)

ZenGo 2023. MPC Wallet. Viitattu 3.2.2023. <https://zengo.com/mpc-wallet/>

#### Julkaisemattomat

Coinmotion 2022. Tiedote korkotilipalvelun käyttäjille. Sähköposti 20.12.2022.

Harju, J. 2022. Asiantuntijahaastattelu 6.12.2022.

Peura, P. 2022. Asiantuntijahaastattelu 13.12.2022.

Piironen, J. 2022. Asiantuntijahaastattelu 8.12.2022.

Runola, V. 2022. Asiantuntijahaastattelu 8.12.2022.

Selosmaa, J. 2022. Asiantuntijahaastattelu 10.12.2022.

Väkeväinen, H. 2022. Asiantuntijahaastattelu 7.12.2022.

Wichmann, M. 2022. Asiantuntijahaastattelu 7.12.2022.

## Kuviot

Kuvio 1: Laitelompakot Coldcard Mk3, Ledger Nano X, Trezor Model T, KeepKey ja BitBox02 (Costea 2019).....	29
Kuvio 2: EK:n yritysturvallisuusmalli (Elinkeinoelämän keskusliitto 2022) .....	33

## Taulukot

Taulukko 1: Asiantuntijahaastattelut .....	41
--	----

## Liitteet

Liite 1: Haastattelukysymykset .....	69
--------------------------------------	----

## Liite 1: Haastattelukysymykset

- Kuka olet ja mitä kokemusta sinulla on kryptovaluutoista?
- Mitä käyttötarkoituksia yrityksillä voisi olla kryptovaluutoilla?
- Mitä riskejä näet kryptovaluuttojen käytössä osana yrityksen liiketoimintaa?
- Voiko yritys hyödyntää GPU-louhintaa osana yrityksen liiketoimintaa?
- Jos GPU-louhinta ei ole palaamassa ennalleen, niin onko ASIC-louhinta vaihtoehto?
- Sopiiko kryptovaluutat osaksi yrityksen hyväksymiä maksutapoja?
- Mitä yrityksen pitäisi tehdä aloittaakseen kryptovaluuttamaksujen vastaanottamisen?
- Miten yrityksen tulisi hallinnoida lompakoita ja yksityisavaimia turvallisesti, jos yrityksellä on useampi osakas tai päättävä taho?
- Miten yrityksen tulisi jakaa lompakoihin pääsy kaikille niitä tarvitseville turvallisesti?
- Mitä yrityksen tulisi tehdä jatkuvuuden kannalta, jos yksi henkilö menehtyy, jolla on pääsy yrityksen kryptovaluuttalompakkoon?
- Mitä yrityksen tulisi tehdä, jos yrityksen kryptovaluuttalompakkoa hallinnoiva henkilö kadottaa yksityisavaimen ja on riski, että se päättyy väärin käsiin?
- Onko hyvää keinoa jakaa yrityksen kryptovaluuttalompakon yksityisavainta usean henkilön kesken yrityksessä?
- Missä tilanteissa Multisig-lompakon käyttö olisi järkevää yrityksessä?
- Mikä on hyvä keino yritykselle säilyttää suuria kryptovaluuttavaroja?
- Onko yrityksillä hyvää keinoa kerryttää korkoa kryptovaluuttavaroilleen?
- Mitä yritys voi tehdä suojellakseen yksityisyyttään suorittaessaan kryptovaluuttatransaktioita, jos yritys ei halua, että siirrot ja lompakon varat ovat kaikille julkisia?
- Ottaen huomioon opinnäytetyöni aiheen, eli kryptovaluuttojen turvallinen käsittely osana osakeyhtiön liiketoimintaa, tuleeko muita asioita tai keinoja mieleen, joiden avulla kryptovaluuttoja voisi käsitellä turvallisemmin yrityksessä?