Kryptovaluutat massarikostutkinnan yhteydessä

Jukka-Pekka Moisio

Haaga-Helia ammattikorkeakoulu
Tradenomi, tietojenkäsittely
Amk-opinnäytetyö
2023

Tiivistelmä

Tekijä(t)
Jukka-Pekka Moisio

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Kryptovaluutat massarikostutkinnan yhteydessä

Sivu- ja liitesivumäärä
52 + 1

Tutkimuksen avulla pyrittiin saamaan aikaan oikea tilannekuva siitä, millaisena kryptovaluuttailmiö näyttäytyy Helsingin poliisilaitoksen rikostorjuntayksikön alaisen rikostutkintayksikön suorittamissa rikostutkinnoissa ja miten hyvin kryptovaluuttojen perustoimintaperiaatteet hallittiin ja tunnistettiin kyseisessä yksikössä.

Tutkimuksessa kerättiin tietoa kryptovaluutoista suorittamalla kirjallisuuskatsaus kohdistuen kryptovaluuttojen perustoimintaperiaatteisiin, historiaan ja käyttöön rikosten yhteydessä. Tutkimuksessa kerättiin tietoa tutkittavan yksikön tilasta asiaan liittyen, suorittamalla haastattelu kahdeksalle rikostutkintayksikön työntekijälle loppuvuodesta 2022. Haastattelun yhteydessä selvitettiin työntekijöiden kokemuksia ja näkemyksiä koskien kryptovaluuttoja sekä selvitettiin kuinka hyvin he hallitsevat kryptovaluuttoihin liittyvät perusasiat ja olivatko he saaneet asiaan liittyvää koulutusta.

Tutkimuksessa käytiin läpi kryptovaluuttojen fyysistä löytämistä tukevaa lainsäädäntöä. Tutkimuksesta rajattiin pois salaisten pakkokeinojen tarkastelu, tietopyyntöjen tarkastelu ja kryptovaluuttojen transaktioiden jäljittäminen. Tutkimuksessa ei käyty läpi taktisen rikostutkinnan menetelmiä, eikä tutkimuksen ole tarkoitus toimia kryptovaluuttoihin kohdistuvan esitutkinnan suorittamisen oppaana.

Tutkimustuloksen perusteella pystyttiin löytämään kehityskohteita tutkitun yksikön toiminnassa. Tutkimuksen tuloksen perusteella voitiin päätellä, että kryptovaluuttojen tunnistamisessa ja niiden perustoimintaperiaatteiden ymmärtämisessä oli kehitettävää. Tutkimuksessa selvisi myös kryptovaluuttojen muodostavan varsin marginaalisen osan tutkitun yksikön työnkuvaa.

Tutkimuksella ei ole toimeksiantajaa. Tutkimuksen tekijä työskenteli tutkimuksen tekemisen aikaan Helsingin poliisilaitoksella, mutta hän ei työskennellyt tutkimuksen kohteena olleessa yksikössä. Tutkimuksen tekijä on kuitenkin työskennellyt tutkitussa yksikössä vuonna 2021. Tutkimuksen teon motiivina toimi tutkimuksen tekijän henkilökohtainen kiinnostus kryptovaluuttoja kohtaan sekä satunnaiset törmäämiset niihin työtehtävien yhteydessä.

Tutkimusta voidaan käyttää tutkitun yksikön toimintatapojen kehittämiseen. Tutkimus tarjoaa ainutlaatuisen näkymän aiheeseen, koska tutkijan tiedossa ei ole, että vastaavan tyyppistä tutkimusta olisi aiemmin tehty.

Asiasanat
virtuaalivaluutta, kryptovaluutta, rikollisuus, poliisi, bitcoin, rikostutkinta

Sisällys

1 Johdanto

Kryptovaluutat ovat usein julkisuudessa koskien niiden väitettyä yhteyttä rikolliseen toimintaan. Itsessään kryptovaluutat ovat vain eri käyttötarkoituksia varten suunniteltujen ohjelmistokokonaisuuksien muodostamia protokollia, mitkä tarvitsevat toimiakseen tietokoneverkoston ja joita käytetään matkapuhelimien tai tietokoneiden avulla. Kryptovaluuttojen käyttämä tekniikka mahdollistaa kuitenkin suhteellisen anonyymin arvon siirtämisen maailmanlaajuisesti henkilöltä toiselle ilman välikäsiä. Tämän vuoksi kryptovaluuttojen tiedostaminen toimiviksi arvonsiirron välineiksi sekä niiden perustoimintamekanismien ymmärtämisellä ja niihin liittyvien asioiden tunnistamisella voi olla tärkeä merkitys rikostutkintojen yhteydessä.

Kryptovaluutat eroavat merkittävästi muista tavoista siirtää arvoa. Perinteisesti arvoa on pystytty siirtämään henkilöltä toiselle joko jonkin fyysisen tavaran kuten kullan tai käteisen rahan avulla tai vaihtoehtoisesti rahaa on siirretty henkilöltä toiselle digitaalisesti esimerkiksi pankkien välityksellä. Mikäli tällaista arvonsiirtoa on tehty rikollisessa mielessä, ovat poliisit tottuneet puuttumaan siihen. Mutta miten puuttua kryptovaluutoilla tehtävään rikolliseen arvonsiirtoon? Jotta kryptovaluuttojen takavarikoiminen ja jäljittäminen voisivat onnistua, täytyy ilmiöön liittyvät perusasiat hallita. Tällaisia hallittavia perusasioita ovat esimerkiksi tieto siitä, mitä etsitään ja mistä etsittävän asian pystyy tunnistamaan.

Tässä tutkimuksessa pyritään selvittämään, nousevatko kryptovaluutat esiin Helsingin poliisilaitoksen rikostorjuntayksikön alaisuudessa toimivan rikostutkintayksikön työnkuvassa ja tunnistavatko yksikön työntekijät kyseisen ilmiön sekä hallitsevatko he kryptovaluuttoihin liittyvät perusasiat.

Rikostorjuntayksikössä tutkitaan suurin osa Helsingin poliisilaitokselle tehtävistä rikosilmoituksista. Kyseisessä yksikössä tutkitaan pääsääntöisesti massarikoksia. Massarikokset ovat ns. tavanomaisia rikoksia, joita tapahtuu päivittäin suhteellisesti eniten ja ne ovat lähtökohtaisesti suhteellisen nopeasti tutkittavia. Esimerkiksi pahoinpitelyä pidetään lähtökohtaisesti massarikoksena, kun taas murha ei ole massarikos. Massarikokset muodostavat suurimman osan poliisin tutkimista rikoksista eli ne ovat rikoksia joihin ihmiset useimmiten törmäävät kohdatessaan rikoksia ja joihin he useimmiten syyllistyvät tehdessään rikoksia. Helsingin poliisilaitoksen rikostorjuntayksikössä tyypillisesti tutkittavia rikosnimikkeitä ovat eriasteiset liikenne, pahoinpitely, varkaus, petos ja huumausainerikokset. Rikostorjuntayksikön työnkuva on kuitenkin moninainen ja rikosnimikkeet vaihtelevat laidasta laitaan. Helsingin poliisilaitoksessa on rikostorjuntayksikön lisäksi myös muita rikostutkintayksikköjä, mitkä ovat kuitenkin keskittyneet tutkimaan jotain tiettyä rikossegmenttiä. Tällaisia yksikköjä ovat esimerkiksi ammattimaista rikollisuutta tutkiva yksikkö ja talousrikoksia tutkiva yksikkö. Kryptovaluutat ovat suhteellisen uusi ilmiö, mutta poliisissa niihin on törmätty jo pidemmän aikaa. Jo vuonna 2015 Helsingin talousrikosten tutkintayksiköstä annettiin Ylelle haastattelu, minkä

yhteydessä kryptovaluutat kerrottiin huomioitavan rikostutkintojen yhteydessä rutiininomaisesti (Salumäki 2015). Poliisiin onkin muodostunut vahvaa osaamista kryptovaluuttoihin ja niiden jäljittämiseen liittyen ja on selvää, että talousrikosten ja törkeiden huumausainerikosten tutkinnan yhteydessä kryptovaluuttoihin törmätään toistuvasti. Tutkimuksessa pyrittiin kuitenkin selvittämään miltä tilanne kryptovaluuttojen suhteen näytti normaalin peruspoliisitoiminnan yhteydessä, josta massarikostutkina muodostaa tärkeän osan.

Ottamatta kantaa siihen, ovatko kryptovaluutat hyviä sijoituskohteita tai käyttökelpoisia tuotteita ne kuitenkin kiinnostavat ihmisiä. Kryptovaluuttojen korkein yhteenlaskettu kokonaismarkkina-arvo on ollut tähän mennessä noin 3 biljoonaa dollaria (Coinmarketcap s.a). Summa vastaa karkeasti noin 30 kertaisesti Suomen valtion budjettia (Valtionvarainministeriö s.a). Onkin todennäköistä, että kryptovaluuttojen yleisyyden ja niiden toimintatavan vuoksi niitä löytyy myös poliisin asiakkaiden hallusta.

Tutkimuksessa kerättiin tietoa kryptovaluutoista suorittamalla kirjallisuuskatsaus kohdistuen kryptovaluuttojen perustoimintaperiaatteisiin, historiaan ja käyttöön rikosten yhteydessä. Tutkimus suoritettiin haastattelemalla kahdeksaa rikostutkintayksikön työntekijää. Haastattelun yhteydessä selvitettiin työntekijöiden kokemuksia ja näkemyksiä koskien kryptovaluuttoja sekä selvitettiin, kuinka hyvin he hallitsivat kryptovaluuttoihin liittyvät perusasiat. Tutkimuksessa käytiin läpi myös kryptovaluuttojen fyysistä löytämistä tukevaa lainsäädäntöä. Tutkimuksesta rajattiin pois salaisten pakkokeinojen tarkastelu, tietopyyntöjen tarkastelu ja kryptovaluuttojen transaktioiden jäljittäminen. Tutkimuksessa ei käyty läpi taktisen rikostutkinnan menetelmiä, eikä tutkimuksen ole tarkoitus toimia kryptovaluuttoihin kohdistuvan esitutkinnan suorittamisen oppaana. Tutkimuksen avulla pyrittiin saamaan aikaan oikea tilannekuva siitä, millaisena kryptovaluuttailmiö näyttäytyi tutkittavassa yksikössä ja miten hyvin se hallittiin sekä tunnistettiin kyseisessä yksikössä. Tutkimuksen tuloksen perusteella voitiin päätellä, että kryptovaluuttailmiön tunnistamisessa ja kryptovaluuttoihin liittyvien perusasioiden hallinnassa oli kehitettävää. Tutkimuksessa selvisi myös, että kryptovaluutat muodostivat varsin marginaalisen osan tutkitun yksikön työnkuvaa.

Tutkimuksella ei ollut toimeksiantajaa. Tutkimuksen tekijä työskenteli tutkimuksen tekemisen aikaan Helsingin poliisilaitoksella, mutta hän ei työskennellyt tutkimuksen kohteena olleessa yksikössä. Tutkimuksen tekijä on kuitenkin työskennellyt tutkitussa yksikössä vuonna 2021. Tutkimuksen teon motiivina toimi tutkimuksen tekijän henkilökohtainen kiinnostus kryptovaluuttoja kohtaan sekä satunnaiset törmäämiset niihin työtehtävien yhteydessä. Tutkimus tarjoaa ainutlaatuisen näkymän aiheeseen, koska tutkijan tiedossa ei ole, että vastaavan tyyppistä tutkimusta olisi aiemmin tehty.

2 Kryptovaluuttojen toiminta

Osiossa käydään läpi kryptovaluuttoihin liittyviä termejä sekä perehdytään kryptovaluuttojen toimintamekanismeihin ja historiaan.

2.1 Kryptovaluuttojen toimintaan liittyviä termejä

2.1.1 Protokolla

Protokollalla tarkoitetaan erilaisten toimintojen sarjoja, joiden tekemisen suorittavat kaksi tai useampi osallinen. Protokollalla on aina alku- ja loppupiste ja jokainen toimi on suoritettava protokollan ennalta määrittämässä järjestyksessä. Kaikkien protokollaa suorittavien tahojen täytyy tuntea protokollan vaiheet ja heidän täytyy olla yksimielisiä protokollan suoritustavasta. Protokollan tulee aina johtaa johonkin päätepisteeseen. (Scheneier 2015, luku 2.) Kryptovaluuttojen yhteydessä protokolla on keskeinen termi, koska se kuvaa parhaiten kryptovaluuttojen toimintaa. Kryptovaluutat koostuvat useiden eri toimijoiden suorittamista toimenpiteistä ja jokaisen toimijan täytyy noudattaa kunkin kryptovaluutan määrittämää protokolla, jotta kryptovaluutan toiminta on mahdollista.

2.1.2 Lohkoketju

Lohkoketjua (blockchain) voidaan pitää eräänlaisena tietokantana, mikä koostuu erillisistä osista eli lohkoista. Lohkot sisältävät jonkinlaista niihin syötettyä tietoa. (Caetano 2015, luku 4.) Jokainen lohko valmistuu jonkin säädetyn parametrin mukaan, minkä jälkeen se lisätään aiemmin luotujen lohkojen jatkoksi. Näin lohkot ketjuuntuvat ja tiedot pysyvät järjestyksessä. Lohkoketjuun tehtyjä kirjauksia ei voi muokata tai poistaa. (Quinones & Nakamoto 2021, 37.) Tiivisteet (hash) mahdollistavat lohkoketjun muuttumattomuuden toteutumisen. Tiivisteiden avulla voidaan lohkon tiedoista muodostaa eräänlainen sormenjälki, mikä yksilöi muodostetun lohkon. Koska muodostetun lohkon tietoihin lisätään tietoja myös lohkoketjun edellisen lohkon tiedoista, tulevat mahdolliset myöhemmät muutokset lohkoketjun tiedoissa esiin, koska jos jotakin lohkon tietoa yritettäisiin lohkoketjussa muuttaa, muuttaisi se myös seuraavien lohkojen tietoja merkittävästi. (Caetano 2015, luku 6.) Lohkoketjujen muuttumattomuuden syytä ja toimintamekanismeja käsitellään tutkimuksessa tarkemmin luvussa 2.5. Muuttumattomuuden taustalla toimivia tiivisteitä käsitellään tarkemmin tutkimuksen luvussa 2.4. Lohkoketjussa näkyvät kaikki siihen aikojensaatossa tehdyt kirjaukset ja lohkoketjut kasvattavat kokoaan jatkuvasti, koska aiempia kirjauksia ei poisteta. Julkisiin lohkoketjuihin tehtyjä kirjauksia pystyy kuka tahansa tarkastelemaan esimerkiksi erilaisten nettipalveluiden kautta. Kryptovaluutta ei ole sama asia kuin lohkoketju, mutta useat kryptovaluutat hyödyntävät toiminnassaan lohkoketjuteknologiaa tai samankaltaisia periaatteita.

2.1.3 Kryptovaluutta

Kryptovaluutat perustuvat usein lohkoketjussa sijaitsevaan avoimeen tilikirjaan, mihin kirjataan tapahtumia. Tapahtumat ovat usein arvon muutoksia kryptovaluutan käyttäjien välillä. (Quinones & Nakamoto 2021, 29.) Kryptovaluutat mahdollistavat myös ns. älysopimusten tekemisen. Älysopimukset ovat ohjelmia, jotka on tallennettu kryptovaluuttojen käyttämään lohkoketjuun ja niitä voidaan suorittaa normaalien ohjelmien tapaan. (Frankenfield 2023a.) Tutkimuksessa käsitellään älysopimuksia tarkemmin luvussa 2.7.2.

Kryptovaluuttojen toimintaa ei säännöstele tai hallitse mikään yksittäinen taho, vaan niiden toiminta perustuu yleensä avoimeen lähdekoodiin ja monimutkaisiin algoritmeihin sekä kunkin kryptovaluutan omaa protokollaa noudattaviin tietokoneverkostoihin. Edellä mainitun vuoksi kryptovaluuttoja kutsutaan hajautetuiksi järjestelmiksi. (Caetano 2015, luku 4.) Kryptovaluuttojen hajautettu toiminta aiheuttaa esimerkiksi sen, että mikäli kryptovaluutan käyttäjä siirtää vahingossa kryptovaluuttaa väärään kryptovaluuttaosoitteeseen ja siirto on vahvistettu, ei siirtoa pysty enää perumaan. Ainoa taho, joka pystyy väärin siirretyt varat palauttamaan, on ne haltuunsa saanut taho. Kryptovaluutat ovat siis käyttäjien hallinnoimia eikä kukaan muu pysty niitä hallitsemaan. Näin ollen esimerkiksi kryptovaluuttojen takavarikoiminen on poliisin toimesta mahdotonta, ellei niiden käyttöön ratkaisevasti liittyvää yksityistä avainta saada ensin poliisin haltuun.

Edellä mainittu mahdollistaa myös sen, että periaatteessa kuka tahansa voi hankkia kryptovaluuttaa. Kryptovaluutan käyttäjän ei tarvitse olla minkään pankin tai muun vastaavan instanssin asiakas, riittää että käyttäjä omaa tietokoneen tai matkapuhelimen, internet yhteyden sekä soveltuvan ohjelmiston. (Quinones & Nakamoto 2021, 29.) Nykyisin kryptovaluutta määritelmä kattaa laajan valikoiman erilaisia protokollia ja jokainen kryptovaluutta toimii omalla tavallaan, vaikka ne usein jakavat samanlaisia piirteitä.

Kryptovaluutat voidaan jakaa karkeasti kolmeen kategoriaan niiden toiminnan ja käyttötavan mukaan. Nämä kategoriat ovat valuutat, alustat ja tokenit. (Hyppönen 2022a.) Kryptovaluuttoihin liittyvä teknologia on vielä suhteellisen uutta ja se kehittyy koko ajan hurjaa vauhtia. Tällä hetkellä käytettävissä olevat ratkaisut voivat korvautua hyvinkin nopeasti uusilla kehittyneemmillä vaihtoehdoilla. Tällä hetkellä kryptovaluuttamaailmaan liittyvät sovellukset ovat vielä varsin kankeita käytettävyydeltään, mutta ne voivat muuttua hyvinkin nopeasti käyttäjäystävällisimmiksi. Tämä voi lisätä kryptovaluuttojen suosiota ja yleisyyttä. Tästä syystä poliisien on syytä seurata kryptovaluuttoihin liittyviä asioita, koska niiden yhteydessä saattaa kehittyä yllättäviäkin käyttötapoja, jotka voivat nousta esiin rikoksiin liittyvinä ilmiöinä.

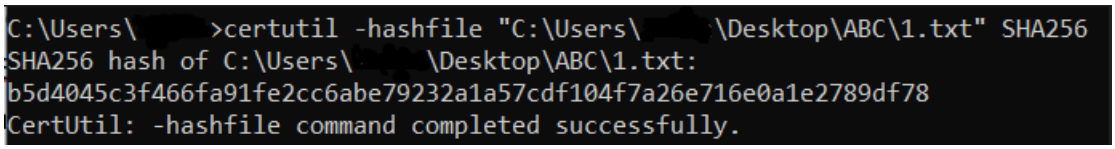
2.1.4 Tiiviste

Tiivisteellä (hash) tarkoitetaan lopputulosta, mikä syntyy tiivistealgoritmin avulla. Tiivistealgoritmille annetaan jokin syöte ja tästä annetusta syötteestä muodostetaan tiivistealgoritmin avulla tulos, mikä on tiivistealgoritmissa määritellyn pituinen. Käytännössä tulos on tiivistealgoritmissa määritellyn pituinen merkkijono. Tiiviste toimii eräänlaisena alkuperäisen syötteen sormenjälkenä, mikä yksilöi syötteen, koska mahdollisia tiivistetuloksia on niin paljon, että erilaisten syötevaihtoehtojen satunnainen kokeileminen vastaavan tiivistetuloksen aikaan saamiseksi on hyvin hankalaa. Edellyttäen, että tiivistealgoritmi on suunniteltu hyvin. Hyvän tiivisteen tunnusmerkkinä on, ettei sen tuottamasta tuloksesta pysty takaisinlaskun avulla muodostamaan alkuperäistä syötettä. Hyvän tiivisteen tunnusmerkkinä on myös se, ettei kahdesta erilaisesta syötteestä muodostu käytännössä koskaan samanlaista tiivistetulosta ja pienikin muutos syötteessä muuttaa syntyvää tiivistetulosta huomattavasti. (Scheneier 2015, luku 18.1.) Tiivisteitä voidaan muodostaa useilla eri tavoilla (Scheneier 2015, luku 18.7). Yleisimmät käytössä olevat tiivisteet ovat tällä hetkellä SHA2, MD5 ja CRC32 nimiset tiivistealgoritmit. Myös RIPEMD160-tiivistealgoritmi on mainitsemisen arvoinen, varsinkin puhuttaessa Bitcoinista, koska sitä ja SHA256-algoritmia käytetään Bitcoinin toiminnan yhteydessä. Tällä hetkellä paljon käytössä olevan SHA-algoritmiperheen on luonut Yhdysvaltojen National Security Agency eli NSA. (Bertaccini 2022, luku 4.) Tiivisteiden perässä oleva luku kertoo usein sen, kuinka pitkä niiden tuottama tiivistetulos on. Esimerkiksi SHA256-algoritmi tuottaa 256 bittiä pitkän tiivistetuloksen mikä vastaa 64:ää heksadesimaalimerkkiä. Aina näin ei kuitenkaan ole esimerkiksi MD5-algoritmin yhteydessä.

Vaikka MD5 ja RIPEMD-algoritmit ovat yhä varsin yleisessä käytössä, on ne havaittu haavoittuviksi. Haavoittuvuus perustuu siihen, että on pystytty osoittamaan, etteivät ne ole törmäysvapaita. Tällä tarkoitetaan sitä, että sama tiivisteen lopputulos on pystytty tuottamaan kahdella erilaisella syötteellä. Tällöin tiivisteen toimiminen alkuperäisen syötteen sormenjälkenä vaarantuu. (Bertaccini 2022, luku 4.)

SHA-algoritmi jakautuu eri versioihin eli SHA1, SHA2 ja SHA3 versioon (Bertaccini 2022, luku 4). SHA1 versio on todettu haavoittuvaksi jo vuonna 2005, eikä sitä tule enää käyttää minkään tärkeän asian tiivistämiseen. Tällä hetkellä esimerkiksi SHA256-tiivistettä pidetään käytössä turvallisena. (Kyberturvallisuuskeskus 2020.)

Alla kuva missä 1.txt tiedoston sisällöstä on muodostettu Windows-käyttöjärjestelmän komentorivillä SHA256-tiiviste. 1.txt tiedoston sisältönä on kirjainyhdistelmä ABC. Tulos on 64 heksadesimaalimerkkiä pitkä lukujono.

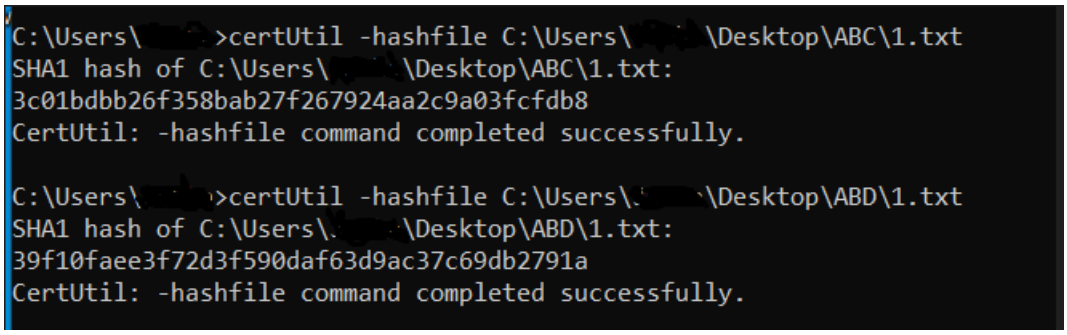


Kuva 1. SHA256-tiiviste

Syntyneessä tiivisteessä on huomioitavaa, että luku on tuotu esiin käyttäen hyväksi heksadesimaalijärjestelmää.

Kymmenjärjestelmässä yhden merkkialkion paikalla voi olla jokin luku 0–9 välillä, kun taas heksadesimaalijärjestelmässä yksi merkkialkio voi olla luku 0–9 välillä tai merkki A-F. Näin ollen eri vaihtoehtoja yhden merkkialkion arvolle löytyy heksadesimaalijärjestelmässä yhteensä 16 kappaletta. (Mocc 2023, luku 3.) Edellä mainitun perusteella voidaan nähdä, että SHA256-tiivisteessä erilaisille syötteille on olemassa valtava määrä erilaisia lopputulos vaihtoehtoja, joten riski tiivistetulosten törmäykselle on pieni.

Alla on kuva, missä käyttäen SHA1-tiivistealgoritmia Windowsin komentorivillä, on kahdesta eri 1.txt nimisestä tiedostosta muodostettu SHA1-tiivisteet. Ylempi tiiviste on muodostettu, kun 1.txt tiedoston sisältönä on ollut kirjainyhdistelmä ABC. Alemmassa sisältönä on ollut kirjainyhdistelmä ABc. Kuten tuloksesta näkyy, pienikin muutos tekstissä muuttaa tiivisteen lopputulosta huomattavasti. SHA1-tiivisteen lopputulos on 160 bittiä eli 40 heksadesimaalimerkkiä pitkä merkkijono. Pidempi tiivistetulos on yleensä turvallisempi käytössä kuin lyhyempi, koska erilaisille syötteille on tarjolla enemmän lopputulos vaihtoehtoja.



Kuva1. SHA1-tiiviste

2.1.5 Julkinen ja yksityinen avain

Julkista ja yksityistä avainta (public and private key) käytetään tiedon salaamiseen sekä tietojen allekirjoittamiseen. Kyseessä on kahden eli julkisen ja yksityisen avaimen muodostama pari, joista yksityinen avain pidetään salassa ja julkinen avain voidaan jakaa julkisesti kaikille. (Caetano 2015, luku 4.)

Julkinen avain muodostetaan yksityisestä avaimesta eli avainten välillä on yhteys. Bitcoinin osalta yksityinen avain muodostetaan valitsemalla satunnaisotannalla suuri luku. Tästä luvusta muodostetaan julkinen avain ECDSA:n eli elliptisen käyrän salausmenetelmän avulla, käyttäen hyväksi Secp256k1 käyrää. Bitcoinin osalta yksityinen avain on 256 bitin eli 64 heksadesimaalimerkin mittainen lukujono. Hyvän julkisen avaimen tunnusmerkkinä on, että siitä on käytännössä mahdotonta matemaattisesti laskea takaisin yksityistä avainta. (Saqan 2022.)

Julkista avainta voidaan hyödyntää viestin salaamisessa. Tällöin viestin lähettäjä salaa viestinsä viestin vastaanottajan julkisella avaimella, jolloin ainoastaan viestin vastaanottaja pystyy purkamaan salauksen yksityisellä avaimellaan. (Frankenfield 2021.)

Viestin allekirjoittaminen taas toteutetaan siten, että viestin lähettäjä allekirjoittaa lähettämänsä viestin, salaamalla viestin yksityisellä avaimellaan. Tämä allekirjoitus voidaan purkaa vain viestin lähettäjän julkisella avaimella. Tällöin viestin vastaanottaja pystyy tarkastamaan viestin lähettäjän allekirjoituksen oikeellisuuden lähettäjän julkisen avaimen avulla. (Saqan 2022.)

Julkinen/yksityinen avainpari on kaiken keskiössä, kun puhutaan kryptovaluutoista. Yksityisen avaimen haltijalla on rajaton käyttöoikeus kaikkiin sen alla oleviin varoihin. Kenelläkään muulla ei tuota valtaa ole.

Alla kuva missä www.bitaddres.org nettisivustolla on avaingeneraattorin avulla luotu julkinen/yksityinen avainpari. Yksityinen avain on kuvan oikeassa alalaidassa näkyvä heksadesimaali merkkijono. Kuvan vasemmassa alalaidassa näkyvä heksadesimaali merkkijono on julkinen avain. Internetissä toimivat avaingeneraattorit eivät ole luotettavia, eikä niitä tule koskaan käyttää merkityksellisten avainten luontiin. Tutkimuksessa nettigeneraattorin luomaan avainparia on käytetty esimerkkinä sen selkeän visuaalisen ulkoasun vuoksi.

Kuva 2. www.bitaddres.org julkinen ja yksityinen avain

2.2 Kryptovaluuttojen historia

Kryptovaluuttojen historiaa ei voi tarkastella ilman, ettei tarkastelisi Bitcoin-kryptovaluuttaa ja sen historiaa. Bitcoin on tällä hetkellä suurin kryptovaluutta ja sen arvon heilahtelut vaikuttavat voimakkaasti myös muiden kryptovaluuttojen arvoon. Bitcoinia voikin tällä hetkellä pitää eräänlaisena kryptovaluuttaindeksinä.

Bitcoin on protokolla, minkä avulla on luotu ensimmäinen hajautettu, yleisesti käytetty digitaalinen kryptovaluutta. Bitcoin perustuu lohkoketjussa sijaitsevaan avoimeen tilikirjaan, mihin merkitään siirtoja eli muutoksia arvon omistajissa. Bitcoineja voidaan tuottaa maksimissaan 21 miljoonaa kappaletta. (Quinones & Nakamoto 2021, 58-61.)

Nimimerkki Satoshi Nakamoto julkaisi verkossa Bitcoin-protokollan esittelyn eli ns. whitepaperin vuonna 2008 ja vuonna 2009 louhittiin ensimmäinen Bitcoin-lohko (Caetano 2015, luku 4). Nakamoto hävisi julkisuudesta melko pian Bitcoinin syntymän jälkeen, eikä kyseinen nimimerkki ole sen koommin esiintynyt missään. Nakamoton henkilöllisyyttä on pyritty selvittämään useasti mutta se on vielä tänäkin päivänä mysteeri. Erilaisia veikkauksia Nakamoton henkilöllisyydestä on esitetty aina eri valtioiden tiedustelupalveluihin asti.

Nakamoton ajatuksena oli kehittää vertaisverkkoa hyödyntävä protokolla, missä arvoa pystyttäisiin siirtämään henkilöltä toiselle ilman, että välissä tarvitsisi luottaa mihinkään kolmanteen yksittäiseen osapuoleen, kuten pankkiin. Nakamoto päätyi esittämään ratkaisua, missä arvonsiirron oikeellisuudesta ja turvallisuudesta huolehtisi Bitcoin-protokollaa noudattava tietokoneverkosto, käyttäen hyväkseen verkoston tietokoneiden laskentatehoa. Palkinnoksi käytetystä laskentatehosta ja siitä aiheutuneista kuluista, siirtojen varmistamiseen osallistuneet tahot voisivat saada haltuunsa bitcoineja. Bitcoin-protokolla määrittele, miten arvonsiirto Bitcoin-verkostossa tapahtuu ja kuinka siirtojen oikeellisuus sekä turvallisuus taataan. (Caetano 2015, Luku 4.)

Bitcoinia pidetään ensimmäisenä kryptovaluuttana mutta ajatus itsenäisestä digitaalisesta valuutasta oli syntynyt jo kauan ennen Bitcoinia. Aluksi asialla oli ns. kyberpunkkariliike. Kyberpunkkariliikkeen toimijat kyseenalaistivat keskitetyn pankkijärjestelmän sekä siihen linkittyvän rahan ja vallan suhteen. Kyberpunkkariliikkeen vaihtoehto perinteiselle keskitetylle pankkijärjestelmälle oli digitaalinen valuutta, mikä ei olisi sidoksissa mihinkään valtioon, valuuttaan tai hyödykkeeseen, eikä tällä digitaalisella valuutalla tulisi olla yksittäistä hallitsijaa, vaan arvon omistajat itse hallitsisivat omaisuuttaan. (Quinones & Nakamoto 2021, 27-28.)

Ensimmäinen kryptovaluutta tyyppinen digitaalinen valuutta kehitettiin valmiiksi jo vuonna 1990 ja se sai nimekseen eCash. ECashia seurasi useita muita projekteja, joissa tuotettiin erilaisia toimintaperiaatteita noudattavia digitaalisia valuuttoja, mutta vasta Bitcoin onnistui saamaan taakseen

merkittävän käyttäjäkunnan. (Reiff 2022.) Bitcoinia seuranneita kryptovaluuttoja kutsutaan altcoineiksi (alternative coin) eli vaihtoehdoksi bitcoinille (Frankenfield 2022a).

Alkuun Bitcoin pysyi pienen joukon projektina, eikä se saanut heti osakseen suurta huomiota. Kuitenkin lokakuussa 2009 bitcoinia ostettiin ensimmäisen kerran perinteisellä rahalla. Osto tehtiin internetpörssissä ja tuolloin 5050 bitcoinia vaihtoi omistajaa 5.02 dollarilla. Bitcoinin hinta määräytyi tuolloin sen louhimiseen eli tuottamiseen käytetyn energian hinnan avulla. Toukokuussa 2010 bitcoineilla suoritettiin ensimmäinen osto, jolloin bitcoineilla ostettiin 25 dollarin arvosta pitsaa. Pitsojen hinnaksi muodostui 10.000 bitcoinia. (Ammous 2018, prologue.) Yhden bitcoinin arvo on ollut tähän mennessä korkeimmillaan noin 68 000 dollaria (Coinmarketcap s.a). Tuolla arvolla laskettuna ostettujen pitsojen hinnaksi muodostuisi noin 680 miljoonaa dollaria. Bitcoin-verkosto kuitenkin tarvitsi näitä ensimmäisiä ostoja todistaakseen toimintansa, eikä pitsojen ostohetkellä pystytty vielä mitenkään näkemään Bitcoinin tulevien vuosien suosiota tai hintakehitystä.

Bitcoinin jälkeen on kehitetty useita uusia kryptovaluuttoja ja kirjoitushetkellä kryptovaluuttoja listaavan Coinmarketcap-sivuton mukaan erilaisia kryptovaluuttoja on kaikkinensa yli 20 000 kappaletta (Coinmarketcap s.a).

2.3 Konsensus

Perinteisesti tietoliikenteeseen perustuvassa tiedonsiirrossa on noudatettu client/server eli asiakas/palvelin -mallia. Tässä mallissa asiakas lähettää palvelimena toimivalle tietokoneelle tietopyynnön ja palvelin vastaa tietopyyntöön toimittamalla asiakkaalle halutun tiedon. (Caetano 2015, Luku 5.) Asiakas voi myös lähettää toimenpidepyyntöjä palvelimelle, jolloin palvelin toimii toimenpidepyynnön mukaan, esimerkiksi tekee toimenpidepyynnön mukaisia muutoksia hallitsemaansa tietokantaan.

Tässä mallissa asiakas ottaa yhteyden palvelimeen, mitä hallitsee jokin auktoriteetti kuten pankki. Tällöin asiakas esimerkiksi käynnistää matkapuhelimessaan pankin sovelluksen, mikä hakee pankin palvelimelta tiedon siitä, paljonko asiakkaan tilillä on rahaa ja tuon tiedon asiakas näkee matkapuhelimensa näytöltä. Tällöin pankki vastaa siitä, että sen kirjanpito pitää paikkansa ja mikäli asiakas suorittaa esimerkiksi maksun toiselle tilille, päivittää pankki tietokantaansa ja ilmoittaa mahdollisesta maksusta toisille pankeille. Tässä mallissa asiakas ei siis itse hallitse varojaan, vaan varojen hallinnointi on pankin vastuulla. Tietenkin asiakas vastaa omien varojen kulutuksesta, mutta konkreettisesti asiakkaan varat ovat lukuja tietokannoissa ja näiden tietokantojen ylläpidosta, käytettävyydestä, eheydestä ja luottamuksellisuudesta vastaa pankki. Tässä mallissa konsensusmekanismina toimii se, että pankki tunnistaa asiakaan luotettavasti, minkä jälkeen pankki vertaa asiakkaan tekemiä toimenpidepyyntöjä omiin tietoihinsa ja toimii keräämiensä tietojen mukaan. Tässä

mallissa on olemassa vain yksi osapuoli eli pankki, joka vastaa varojen hallinnoinnista, jolloin asiakkaan luottamus pankin toimintaa kohtaan mahdollistaa mallin toiminnan.

Kryptovaluutat eivät toimi perinteisen asiakas/palvelin -mallin mukaan, vaan ne toimivat vertaisverkostona mikä koostuu asiakkaista. Kryptovaluuttojen toimintaa voisi kuvata client/client eli asiakas/asiakas -malliksi. Tässä mallissa asiakkaat eivät lähetä tietopyyntöjä palvelimelle, vaan he lähettävät tietoa ja toimenpidepyyntöjä toisille asiakkaille ja ne saavat tietoa toisilta asiakkailta. Näitä tietoja levitetään verkoston kaikille osallisille. (Caetano 2015. Luku 5.) Tässä mallissa luottamuksen takaava konsensusmekanismi täytyy rakentaa eri tavalla kuin perinteisessä asiakas/palvelin -mallissa.

Kryptovaluuttojen toimintamekanismissa ei siis luoteta yhteen tahoon kuten pankkiin ja siihen, että pankin tiedot pitävät paikkansa. Kryptovaluutoissa luottamus tietojen paikkansa pitävyydestä liittyy siihen, että kaikki osalliset pystyvät tarkastamaan mikä tieto on tosi. (Nakamoto. 2008. s.2.) Kryptovaluutat ovat hajautettuja järjestelmiä, joissa verkoston kaikki osalliset eivät saa kaikkea tietoa tai viestejä yhtä aikaa eli hajautetut verkostot eivät tässä mielessä toimi reaaliaikaisesti (Li & Wang 2022). Kryptovaluuttojen osalta yhteisymmärrykseen päästään sillä, että kaikki hyväksytysti luotu kryptovaluutta ja sen suhteen tehdyt hyväksytyt siirrot ovat kaikkien osallisten tarkistettavissa. On siis olemassa yhteisymmärrys siitä, mistä asian voi tarkistaa ja milloin tämä tieto on luotettavaa (Caetano 2015, Luku 4.) Se millaisten mekanismien avulla tällaista luotettavaa tietoa pystytään tuottamaan, määritellään jokaisen protokollan kohdalla erikseen. Tutkimuksen luvussa 2.5 käsitellään tarkemmin mekanismeja, joiden avulla tällainen luotettava tieto voidaan saada aikaiseksi.

Mikäli konsensusmekanismeja ei olisi käytössä, mahdollistaisi se ns. kaksoislaskutuksen (double-spending problem). Bitcoin-kryptovaluutan ns. bigspender-haavoittuvuus kuvastaa hyvin kaksoislaskutus-ongelmaa. Bigspender ei varsinaisesti ole kaksoislaskutusta, koska Bitcoinin konsensusmekanismi toimii sen yhteydessä oikein. Bigspender on Bitcoin-protokollan ominaisuuksia hyödyntävä huijaus, mikä on tehty kaksoislaskutuksen periaatteita mukaillen. Mikäli konsensusmekanismia ei olisi, pystyttäisiin vastaavanlaisia siiroja tekemään hyväksytysti, eikä protokolla voisi toimia.

Bigspenderiä käytettäessä huijaaja lähettää bitcoineja uhrille esimerkiksi maksuna jostain tavarasta. Bitcoinia lähetettäessä täytyy maksaa siirtomaksu, jotta siirtoja varmistavat ns. louhintasolmut ottavat siirron käsiteltäväkseen eli vahvistettavakseen. Mikäli siirtomaksu on liian pieni, eivät louhintasolmut ota siirtoa käsiteltäväkseen. Yksinkertaistaen bigspenderiä käytettäessä huijaaja lähettää kaikki bitcoin varansa tilittään uhrin tilille ja maksaa tässä yhteydessä liian pienen siirtomaksun, jolloin louhintasolmut eivät ota kyseistä siirtoa käsiteltäväkseen. Kyseisenlainen siirto näkyi kuitenkin joissain kryptovaluuttalompakoissa siten, että uhri saattoi luulla siirron tulleen läpi. Huijaajat tekivät kuitenkin välittömästi ensimmäisen siirron jälkeen uuden siirron toiseen mutta

itsensä omistamaan kryptovaluuttalompakkoon, maksaen tuon siirron yhteydessä suuremman siirtomaksun. Suuremman siirtomaksun vuoksi louhintasolmut ottivat myöhäisemmän siirron heti käsiteltäväkseen. Näin myöhemmin tehty siirto hyväksyttiin ja vahvistettiin ensin ja vain se merkittiin Bitcoinin kirjanpitoon, eikä ensimmäinen siirto tullut koskaan läpi, koska lähettävän osoitteen varat oli jo kulutettu. (ZenGo 2020.)

2.4 Kryptovaluuttojen toimintamekanismit

Kryptovaluuttojen suuren määrän vuoksi ei ole mahdollista antaa tarkkaa kuvaa kyseisen ilmiön toimintatavasta. Jokainen kryptovaluutta toimi aina hieman omalla tavallaan ja ne on kehitetty eri käyttötarkoituksia silmällä pitäen. Usein kryptovaluuttoja kutsutaan projekteiksi, koska ne perustuvat avoimeen lähdekoodiin ja kuka tahansa voi kehittää niitä eteenpäin. Kryptovaluuttojen kehityksenhallinnan suhteen on kehitetty erilaisia ratkaisuja kuten äänestysratkaisuja mutta niiden tarkastelu on rajattu tutkimuksesta pois asian laajuuden vuoksi. Kryptovaluuttojen toimintaa voidaan kuitenkin tarkastella yleisellä tasolla, ottamalla kohteeksi kaksi erityyppistä ja yleisesti käytettyä kryptovaluuttojen toiminta- ja konsensusmekanismia. Nämä toimintamallit ovat proof of work (PoW) ja proof of stake (PoS). Tutkimuksessa käytetään näistä toimintamalleista vapaita suomennuksia, missä proof of work = työtodennus ja proof of stake = panokseen perustuva todennus. Bitcoin noudattaa työtodennus toimintamallia ja kirjoitushetkellä toisiksi suurin kryptovaluutta Ethereum noudattaa panokseen perustuvan todennuksen toimintamallia.

2.5 Työtodennus

Tutkimuksen seuraavassa luvussa esitellään kryptovaluuttojen toimintaa osin Bitcoinin avulla, jotta asiasta saadaan helpommin ymmärrettävä. Bitcoinin toiminnan ymmärtäminen auttaa myös muiden kryptovaluuttojen toiminnan ymmärtämistä, koska yleensä niiden toimintatavat ovat pääperiaatteiltaan samankaltaisia. Bitcoin perustuu avoimeen lähdekoodiin ja sen lähdekoodi on tarkasteltavissa GitHub-versionhallintajärjestelmässä osoitteessa https://github.com/bitcoin/bitcoin.

Bitcoin-verkosto koostuu ns. solmuista (node). Solmut tarkoittavat tietoteknisiä laitteita kuten tietokoneita tai niiden verkostoja, joiden resursseja on valjastettu suorittamaan jotain tiettyä toimintaa. Solmutyypeistä kolme on merkittävintä. (moreReese 2022.) Tutkimuksessa käytetään näistä solmuista niiden toimintatavan mukaan nimettyjä vapaita suomennuksia seuraavasti, louhintasolmut, täydet solmut ja kevyet solmut.

Mikäli joku haluaa liittyä Bitcoin-verkostoon, täytyy hänen ensin asentaa tietotekniselle laitteelleen sopiva ohjelmisto. Ladattu ohjelmisto mahdollistaa Bitcoin-verkoston solmuna toimimisen. Kun ohjelma on asentunut ja sitä ryhdytään käyttämään, ottaa ohjelmisto yhteyden toisiin Bitcoin-

verkoston solmuihin ja vaihtaa niiden kanssa tietoja. Tätä kautta Bitcoin-verkoston käyttäminen on mahdollista. (Caetano 2015, luku 5.)

Solmutyypeistä täydet solmut säilyttävät koko Bitcoin-lohkoketjun tietoja eli yhteisesti jaettua tietokantaa minkä voi nähdä myös yhteisesti jaettuna tilikirjana, johon on talletettu kaikki Bitcoin-verkostossa aiemmin tapahtuneet toimenpiteet eli käytännössä arvonsiirrot. Nämä arvonsiirrot on tallennettu tilikirjaan osina eli lohkoina. Yksi lohko voi pitää sisällään tuhansia siirtoja. Täydet solmut tarkastavat Bitcoin-verkostoon kuulutettujen uusien siirtojen sekä uusien muodostettujen lohkojen oikeellisuuden, ennen kuin ne hyväksyvät siirrot ja muutokset jaetussa tietokannassa ja jakavat tiedon eteenpäin muille solmuille. (moreReese 2022.)

Kevyet solmut eivät tallenna täyttä versiosta Bitcoinin-tilikirjasta vaan niiden versio on kevyempi ja niiden täytyy varmistaa täysiltä solmuilta omien tietojensa paikkansapitävyys. Kryptovaluuttoihin liittyvät lompakkosovellukset voivat toimia kevytsolmuina. (moreReese 2022.)

Louhintasolmut keräävät Bitcoin-verkostoon kuulutettuja siirtoja kasaan lohkoihin mitkä ne yrittävät matemaattisen kilvan voittamalla validoida. Louhintasolmut yrittävät siis päästä merkitsemään oman lohkonsa tiedot Bitcoinin-tilikirjaan. Louhintasolmut käyvät tätä kisaa muita Bitcoin-verkoston louhintasolmuja vastaan. Tätä toimintaa kutsutaan louhimiseksi. Mikäli louhintasolmu voittaa kisan, saa se palkinnoksi lohkonluonnin yhteydessä luotuja uunituoreita bitcoineja sekä sen validoiman lohkon siirtojen yhteydessä maksetut siirtomaksut. (Caetano 2015, luku 6.)

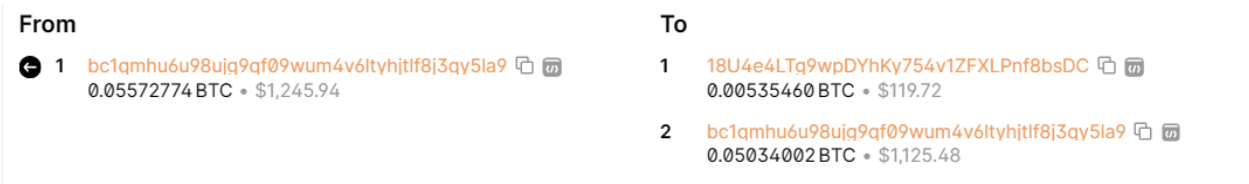
Louhintakilpailu vaatii nykyisin valtavan määrän laskentatehoa ja louhintatoiminta onkin pitkälti ammattilaisten suorittamaa toimintaa varsinkin Bitcoinin osalta. Käytännössä se kenellä on eniten laskentatehoa käytössään, pystyy pitkällä aikavälillä validoimaan suurimman määrän lohkoja ja voittamaan eniten bitcoineja itselleen. (Frankfield 2022b.) Kryptovaluuttojen taustalla toimii erilaisia toimijoita, joilla on mahdollisuuksia vaikuttaa eri kryptovaluuttojen toimintaan, mutta näiden tahojen tarkastelu on rajattu tutkimuksesta pois asian laajuuden vuoksi.

Miten kryptovaluuttaa sitten syntyy tässä toimintamallissa? Kuten todettua Bitcoin-kryptovaluutta koostuu lohkoista. Ensimmäinen lohko on erityistapaus ja se on syntynyt tavallaan tyhjästä ja onkin helpompaa tarkastella Bitcoinin toimintaa ensimmäisen lohkon luomisen jälkeen. Hyväksykäämme siis lähtökohdaksi se, että Bitcoinin ensimmäinen lohko on luotu ja bitcoinia on päätynyt eri tahojen haltuun.

Henkilöllä A on nyt siis hallussaan bitcoinia. Henkilö A haluaa siirtää osan hallussaan olevasta bitcoinista henkilölle B. Ensimmäiseksi henkilön A täytyy selvittää henkilön B kryptovaluuttatilin osoite. Tuona osoitteena toimii yksinkertaistettuna henkilön B julkisen/yksityisen avainparin julkinen avain.

Henkilö A ilmoittaa siirtävänsä tietyn osan hallussaan olevasta bitcoinista henkilön B julkisen/yksityisen avainparin alaisuuteen. Ilmoituksen hän tekee kuuluttamalla asian maailmanlaajuisesti protokollaa käyttävälle tietokoneverkostolle kryptovaluuttalompakkonsa ohjelmiston avulla. Täydet solmut varmistavat siirron oikeellisuuden ja jakavat tietoa siirrosta eteenpäin. Tieto saavuttaa myös louhintasolmut. Verkosto tietää siirron olevan luvallinen, koska A salaa siirron yksityisen avaimensa avulla ja vain hänellä on tiedossa yksityisen avaimen tiedot, joten siirron täytyy näin ollen olla tosi. Siirron oikeellisuus varmistetaan henkilön A julkisen avaimen avulla. (Ammous 2018, Luku 8.) Henkilön A täytyy maksaa pieni siirtomaksu siirron yhteydessä, eli osa siirretystä kryptovaluutasta kuluu siirtomaksuun.

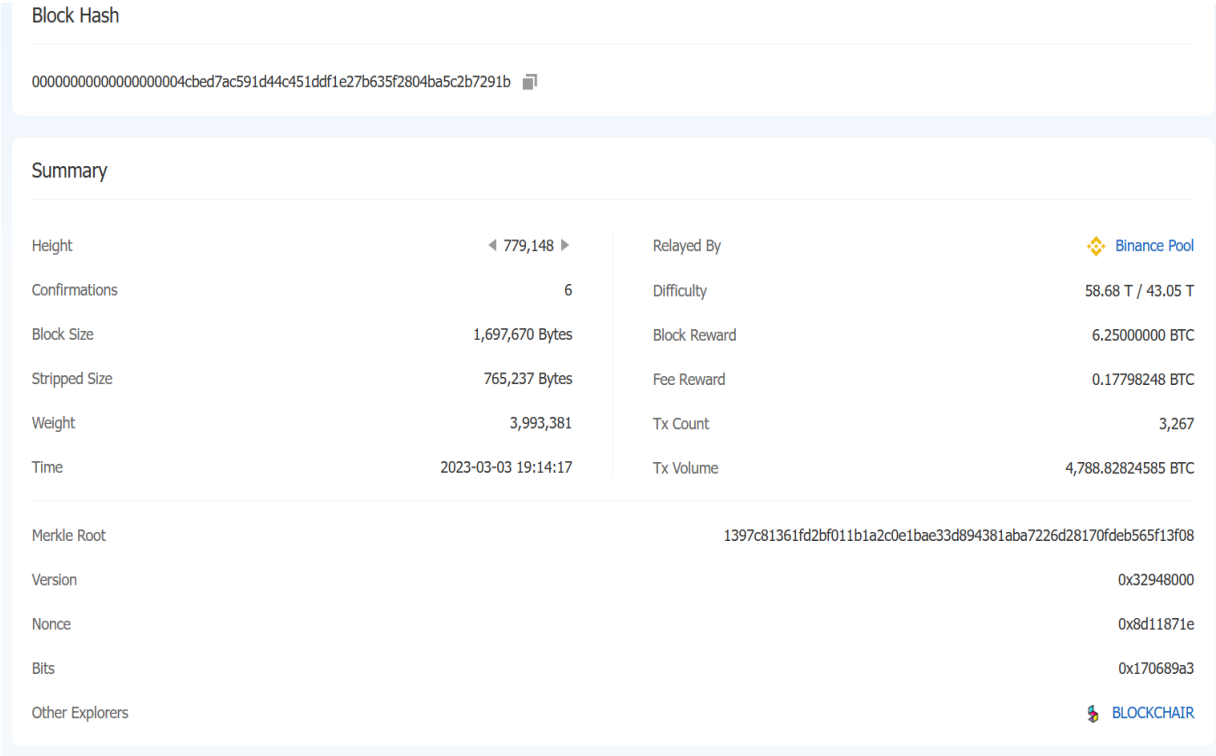
Alla on kuva www.blockchain.com verkkopalvelusta, missä voidaan tarkastella eri lohkoketjujen tapahtumia reaaliaikaisesti. Alla olevassa kuvassa näkyy, kuinka Bitcoin-protokolla käsittelee siirtoja kirjanpidossaan. Vasemmanpuoleisesta Bitcoin-osoitteesta on lähetetty 119.72 dollarin arvosta bitcoineja toiseen Bitcoin-osoitteeseen. Vasemmanpuoleinen numero 1 ja oikeanpuoleinen numero 2 ovat sama osoite eli oikeanpuoleinen ylimmäinen siirto on mennyt uuteen osoitteeseen, ja jäljelle jääneet bitcoinit ovat palanneet kirjanpidossa vanhaan osoitteeseen.



Kuva 3. Blockchain.com kuva bitcoin siirrosta

Louhimisessa louhintasolmut muodostavat edellisen lohkoketjuun tallennetun ja hyväksytyn lohkon tiedoista sekä uusista siirroista ja satunnaisluvusta uuden tiivisteen. Protokolla määrittelee uudelle lohkotiivisteelle tietyt kriteerit, joiden pitää täyttyä, jotta uusi lohkotiiviste hyväksytään. Louhintasolmut yrittävät siis satunnaislukua vaihtamalla saada lohkon tiedoista aikaan hyväksytyn tiivisteen. Tätä oikean satunnaisluvun arvaamista kutsutaan louhimiseksi. (Caetano 2015. Luku 6.)

www.btc.com on toinen verkkopalvelu, missä voi tarkastella Bitcoinin-lohkoketjun tapahtumia reaaliaikaisesti. Alla on kuva www.btc.com palvelusta, missä on yhteenveto yhden muodostuneen lohkon tiedoista.



Kuva 4. Btc.com kuva siirron tiedoista.

Kuvassa ylimpänä näkyy oikea tiivistearvo mikä on saavutettu arvaamalla oikein kuvassa näkyvä nonce eli satunnaisluku siten, että sen sekä lohkon sisältämien tietojen avulla on pystytty muodostamaan kyseinen tiivistearvo. Kyseinen tiivistearvo täyttää lohkonluomisen edellytykset. Protokolla määrittelee lohkoketjussa saatavilla olevan laskentatehon mukaan oikean tiivistearvon aloittavien nollien määrään ja tätä kautta se säätelee louhimisen haastavuutta. Mitä enemmän tiivisteen alkuun vaaditaan nollia, sen haastavampaa uuden lohkon muodostaminen on. (Caetano 2015. Luku 6.)

Se louhintasolmu, joka pystyy arvaamaan satunnaisluvun oikein, pystyy kuuluttamaan saavutuksena Bitcoin-verkostoon. Mikäli muut verkoston osalliset hyväksyvät uuden lohkon, ryhtyvät ne tuottamaan uusia lohkoja sen jatkoksi ja louhintakilpailun voittanut louhintasolmu saa palkinnoksi protokollassa määritellyn määrän kryptovaluuttaa sekä päälle vielä siirtomaksut. Tässä yhteydessä siis syntyy uutta kryptovaluuttaa kiertoon, kun louhintasolmujen hallitsijat saavat haltuunsa louhintapalkkion uuden lohkon muodostamisesta. (moreReese 2022.)

Koska jokainen uusi lohko muodostetaan käyttäen hyväksi myös edellisen lohkon tietoja, ei hyväksytyn lohkon tietoja pysty enää jälkikäteen muuttamaan. Pienikin muutos jossain lohkossa muuttaisi kaikkia seuraavia lohkoja radikaalisti.

Bitcoinit eivät häviä lohkoketjun sisältä mihinkään, vaan ne pysyvät lohkoketjun kirjanpidossa. Lohkoketjuun merkitään ainoastaan kryptovaluutan omistajan muutokset ja louhinnan seurauksena syntyneen uuden kryptovaluutan omistaja.

Kryptovaluuttojen inflaatio voi hidastua pikkuhiljaa, jolloin louhintapalkkio pienenee ajansaatossa. Bitcoinin osalta louhintapalkkio pienennee noin 4 vuoden välein ja enimmillään bitcoineja pystytään louhimaan 21 miljoonaa kappaletta. (Ammous 2018, luku8.) Keskusteluissa onkin pyöritelty, miten Bitcoin-verkosto pystyy toimimaan, kun sitä ei enää pysty louhimaan.

Edellä kerrottu on hyvin yleisellä tasolla annettu kuvaus työtodennus toimintatavasta ja todellisuudessa kyseessä on todella monimutkainen järjestelmä.

2.6 Panokseen perustuva todennus

Proof of stake eli panokseen perustuva todennus perustuu siihen, että siirtojen varmistukseen osallistuvat tahot hankkivat itselleen kyseistä kryptovaluuttaa ja he lukitsevat riittävän määrän kryptovaluutta panokseksi arvontaan, minkä voittaja saa varmistaa kyseisen kryptovaluutan siirroista muodostuneen lohkon (Napoletano 2023). Arvonnan voittaja saa siis päivittää kryptovaluutan tietokantaa keräten samalla yleensä siirtomaksut palkkioksi itselleen (Frankenfield 2023b).

Tässä mallissa kryptovaluutta syntyy ensivaiheessa kahdella eri tavalla. Ensimmäisen tapa on se, että protokolla on ensin noudattanut työtodennusmallia, mistä on sitten siirrytty panokseen perustuvaan todennukseen. Toinen ensivaiheen tapa luoda kryptovaluuttaa tässä mallissa on, että se kirjoitetaan protokollan koodiin, ilmoittamalla kuinka paljon kyseistä kryptovaluuttaa luodaan ja miten sitä pystyy syntymään mahdollisesti lisää. Tämän jälkeen kyseistä kryptovaluuttaa pyritään jakamaan eteenpäin määriteltyjen mekanismien mukaan.

Tässäkin tapauksessa otetaan tarkastelun lähtökohdaksi se, että kyseistä kryptovaluuttaa on päätynyt eri tahojen haltuun ja protokolla toimii. Mikäli joku taho on hankkinut riittävän määrän kyseistä kryptovaluuttaa, pystyy hän osallistumaan siirtojen varmistukseen ja konsensuksen luomiseen.

Tässä mallissa varmistussolmut, joita voisi verrata työtodennuksen louhintasolmuihin eivät käy louhintakilpailua keskenään vaan ne osallistuvat arvontaan, missä protokolla päättää mikä arvontaan osallistuneista varmistussolmuista saa vahvistaa uusista siirroista muodostuneen lohkon tai verkoston tilan, kunkin protokollan määrittämien ohjeiden mukaan. (Saad, Qin, Ren, Nyang & Mohaisene 2021.)

Yleensä panokseen perustuvassa todennuksessa vallitsee käytäntö, missä sillä varmistussolmulla, jolla on eniten panosta lukittuna, on myös suurin mahdollisuus voittaa arvonta. Toinen arvonnan

voittoon vaikuttava seikka on yleensä sillä, kuinka kauan varat ovat olleet lukittuna arvontakisassa. (Saad ym. 2021.) Usein on vielä tapana, että mikäli jokin varmistussolmu voittaa arvonnan, ei se heti pysty osallistumaan arvontaan uudelleen. Tällä pyritään estämään se, että esim. suurimman panoksen asettanut varmistussolmu voittaisi kisan aina eli pyritään turvaamaan verkoston hajaantuneisuus.

Mikäli protokolla havaitsee, että jokin varmistussolmuista on toiminut virheellisesti tai epärehellisesti, on seurauksena yleensä se, että osa tai kaikki varmistussolmun arvontakisaan lukitsemista varoista viedään siltä, eikä se enää mahdollisesti pysty osallistumaan varmistustoimintaan (Blocknative 2022).

Panokseen perustuvassa todennuksessa varmistussolmut saavat korvauksen panostuksestaan yleensä siirtomaksujen muodossa, joita siirtojen tekijät joutuvat maksamaan siirtojen yhteydessä (Saad ym. 2021). Yleensä on tapana, etteivät varmistussolmut saa siirtomaksuja heti hallintaansa vaan vasta jonkin ajan jälkeen. Tällä pyritään varmistamaan, että mahdolliset väärinkäytökset havaitaan ennen palkkionmaksua.

Panokseen perustuvan todennuksen avulla pystytään yleensä saavuttamaan huomattava etu lohkojen luonnin nopeudessa verrattuna työtodennukseen. Yleensä panokseen perustuva todennus myös kuluttaa huomattavasti vähemmän energiaa, kun sitä verrataan työtodennukseen. (Saad ym. 2021.)

Edellä mainitut tavat ovat kuitenkin vain kaksi yleistä toimintamallia, joiden avulla kryptovaluutat toimivat ja niiden lisäksi on olemassa myös suuri joukko muita toimintamalleja.

2.7 Kryptovaluutta kategoriat

Kryptovaluutat voidaan tällä hetkellä jakaa karkeasti kolmeen eri kategoriaan niiden toiminnan ja käyttötavan mukaan. Nämä kategoriat ovat valuutat, alustat ja tokenit. (Hyppönen 2022a.)

2.7.1 Valuutat

Useat kryptovaluutat toimivat perinteisen rahan tapaan, jolloin niiden pääsääntöinen käyttökohde on arvon säilyttäminen ja vaihdon välineenä toimiminen. Esimerkiksi bitcoinia voisi verrata tällä hetkellä rahaan tai ehkä paremmin kultaan. Bitcoinin pääasiallinen tarkoitus on siis toimia arvonvälittäjänä tai säilyttäjänä (Hyppönen 2022a.) Lupaus arvonsäilytyksestä liittyy siihen, että bitcoinit ovat harvinaisia, koska bitcoineja voidaan protokollan mukaan tuottaa vain 21 miljoonaa kappaletta ja niiden tuottaminen vaatii suuren satsauksen riittävän laskentatehon aikaansaamisen myötä.

Myös useat muut kryptovaluutat toimivat valuuttojen tapaa, esimerkkinä Litecoin niminen kryptovaluutta.

2.7.2 Alustat

Osiossa tarkastellaan alustana toimivien kryptovaluuttojen toimintaa selkeyden vuoksi pitkälti Ethereum-kryptovaluutan kautta.

Alustana palvelevat kryptovaluutat toimivat siten, että itse protokolla toimii siirtojen varmistus- ja kuljetuskerroksena ja niiden päälle pystytään rakentamaan hajautettuja ohjelmia, joita kutsutaan älysopimuksiksi. Itse kryptovaluuttaa kolikoita käytetään tässä tapauksessa tiedonsiirroista ja tietokoneverkoston käytöstä aiheutuvien kulujen maksumekanismina. Alustat toimivat jaettuina tietokoneina, joihin voidaan ladata jaettuja ohjelmia ja näitä ohjelmia voidaan suorittaa käyttäjien lähettämien viestien avulla. Alustoina toimivissa kryptovaluutoissa ei päivitetä lohkoketjussa toimivaa jaettua tilikirjaa Bitcoinin tapaan, vaan lohkoketjun tilikirja toimii jaettuna tietoisuutena jaetun tietokoneen kulloisestakin tilasta. (Ethereum 2023d.)

Älysopimuksia on luotu useisiin eri käyttötarkoituksiin, ja ne toimivat kukin sen mukaan, mitä niiden koodiin on kirjoitettu. Alustana toimivat kryptovaluutat tallettavat älysopimusten koodin jaettuun tietokantaansa eli tällöin tapahtuu muutos jaetun tietokoneen tilassa. Mikäli joku käyttää talletettua älysopimusta antamalla sille viestillä käskyn, suorittavat alustana toimivat kryptovaluutat älysopimusten koodin antamalla verkoston laitteistoresursseja älysopimuksen käyttöön sekä turvaavat sen oikeaoppisen suorittamisen. Alustana toimivat kryptovaluutat toimivat siis ikään kuin tietokoneina ja käyttöjärjestelminä, joiden päällä käyttäjien tekemiä ohjelmia ajetaan. (Ethereum 2023a.)

Tunnetuin alustana toimiva kryptovaluutta lienee Ethereum. Ethereumin älysopimuksilla on osoite, mutta niillä ei ole yksityistä avainta. Kun älysopimus on liitetty Ethereum-lohkoketjuun, ei sitä pysty jälkikäteen muuttamaan eikä oletuksena poistamaan. Itse älysopimukseen voidaan kuitenkin liittää koodillisesti toiminnallisuutta normaalin ohjelmoinnin tapaan, jolloin älysopimuksen kanssa pystytään kommunikoimaan. Älysopimukselle annettavat käskyt lähetetään sen osoitteeseen. (Ethereum 2022.)

2.7.3 Tokenit

Tokeneita luodaan älysopimuksen kautta. Token on muuttumaton yksikkö, mikä kuvaa jotakin asiaa, kuten esimerkiksi valuuttaa, mutta oikeastaan vain mielikuvitus on rajana sille, mitä tokenilla voidaan kuvata. Tokeneita on jaoteltu eri käyttötarkoitusten mukaan ja esimerkiksi Ethereumin osalta on luotu standardeja, mitkä määrittävät erilaisten tokeneiden toimintaa. (Binance 2023a.)

Ehkäpä tunnetuin Ethereumin-tokeneita koskeva standardi on ECR-20-standardi. Sen yhteydessä puhutaan fungible tokens -termistä. Tämä termi tarkoittaa sitä, että ERC-20-standardin mukaan kirjoitettujen älysopimusten lopputuloksena on ohjelma, minkä avulla pystytään tuottamaan jotain yhtä samanlaista lopputulosta, käytännössä yksilöivää numerosarjaa ja sen kopioita. Tuota numerosarjaa eli tokenia voidaan sitten lähettää esimerkiksi kryptovaluuttalompakosta toiseen. (Ethereum 2023b.)

Esimerkkinä voitaisiin koodata älysopimus, minkä avulla jaettaisiin yhden kultaharkon omistus kymmeneen yhtä suureen osaan ja jokaista kultaharkon osaa kuvaisi yksi token. Jos joku hankkisi yhden tokenin, omistaisi hän tuolloin 1/10 osan kyseisestä kultaharkosta.

Toisena esimerkkinä voidaan esittää tilanne missä Ethereum-kryptovaluutan päällä luodaan ERC-20-standardin avulla älysopimus, mikä kuvastaa kryptovaluuttaa tokeneiden muodossa. Kuvitteellisessa esimerkissämme kryptovaluutta nimetään markaksi. Älysopimukseen määritellään, että markkoja luodaan 1000 kappaletta, eikä niitä pystytä tuottamaan enempää. Jokainen näistä luoduista markoista on ominaisuuksiltaan samanlainen eli ne ovat toistensa kopioita. Mikään markoista ei ole sen arvokkaampi kuin mikään toinen luotu markka, eikä mikään markoista sisällä muista markoista poikkeavia ominaisuuksia.

ERC-20-standardin tokenit ovat siis keskenään aina samanlaisia ja ne kuvastavat samaa asiaa. Kryptovaluuttojen yhteydessä onkin puhuttu paljon tokenisoinnista, millä nähdään olevan suuri potentiaali tulevaisuudessa, koska nähdään, että erilaisia reaalimaailman asioita voidaan tokenisoida ja näillä tokeneilla voitaisiin käydä kauppaa maailmanlaajuiset.

ERC-20-standardin lisäksi on olemassa myös koko joukko muita ERC-standardeja. Poliisityön kannalta on syytä tunnistaa ERC-20-standardin lisäksi myös toinen merkittävä ERC-standardi eli ERC-721.

Kyseinen standardi koskee non-fungible-tokeneja joiden lyhenne on NFT. NFT on kuvaus jostakin yksittäisestä uniikista asiasta (Ethereum 2023c). NFT:llä voi olla huomattava rahallinen arvo ja ne voivat osoittaa omistusoikeutta esimerkiksi johonkin digitaaliseen taideteokseen tai vaikkapa oikeutta jonkin musiikkikappaleen tekijänoikeuksiin. NFT-tokeneilla nähdään myös olevan suuri potentiaali tulevaisuudessa ja niille kehitetään jatkuvasti uusia käyttötarkoituksia.

Viime vuonna Brussels Times uutisoi, kuinka poliisit olivat rikostutkinnan yhteydessä takavarikoineet kryptovaluuttaa sekä NFT-tokeneita (Lyons 2022). Pitäisinkin todennäköisenä, että tämän tyyppiset NFT-tokeneihin kohdistuvat takavarikot tulevat lisääntymään jatkossa.

3 Kryptovaluutan säilyttäminen ja hankkiminen

Osiossa käydään läpi, miten kryptovaluuttaa pystyy hankkimaan ja kuinka sitä pystyy säilyttämään. Osiossa käydään lyhyesti läpi myös kryptovaluuttapörsseihin liittyviä rikoksia ja huijauksia.

3.1 Lompakot

Kryptovaluuttaa on perinteisesti säilytetty ns. lompakoissa. Lompakot luokitellaan kuumiin tai kylmiin. Myös tällä saralla on viime aikoina tapahtunut nopeaa kehitystä ja nyt käytössä olevat lompakkotyypit voivat vaihtua hyvinkin nopeasti hieman erilaista toimintatapaa eli älysopimuksia noudattaviin ratkaisuihin. Tutkimuksessa käydään kuitenkin läpi perinteisen mallin mukaan toimivat lompakot. Perinteiset kryptovaluuttalompakot ovat yksityisen/julkisen avaimen muodostamia pareja.

3.1.1 Kuumat lompakot

Kuumat lompakot ovat sovelluksia, joilla hallitaan kryptovaluuttaan liittyvää yksityistä avainta, mikä mahdollistaa kryptovaluutan toiminnan. Kuumat lompakot voivat toimia esimerkiksi sovelluksena tietokoneen työpöydällä, nettiselaimen laajennusosana tai älypuhelinsovelluksena. Tällöin ohjelma ladataan laitteelle. ja sen avulla kryptovaluuttoja pystyy suhteellisen helposti hallitsemaan. Tunnettuja kuumia lompakkoja ovat mm. Metamask ja Trustwallet nimiset sovellukset. (Hyppönen 2023b.) Normaalisti kyseisiin sovelluksiin kirjaudutaan sisään salasanalla. Mikäli henkilöllä on tiedossaan kryptovaluuttaan liittyvä yksityinen avain eli se on jo luotu, pystytään se lisäämään kyseistä kryptovaluuttaa tukevaan kuumaan lompakkoon.

Kun sovellus otetaan käyttöön, tarjoaa se luonnin yhteydessä siemenlauseet, joiden avulla voidaan palauttaa sovelluksen luomat julkisten/yksityisten avainten tiedot toiselle laitteelle, mikäli esimerkiksi puhelin mikä sisältää lompakkosovelluksen rikkoutuu. Siemenlauseet ovatkin todella tärkeässä roolissa kryptovaluuttojen ekosysteemissä, eikä niitä tulisi koskaan paljastaa ulkopuoliselle, koska niiden avulla kuka tahansa pystyy pääsemään internetyhteyden avulla käsiksi lompakkoon linkitettyihin yksityisiin avaimiin. (Hyppönen 2023b.)

Alla esimerkki kuvitteellisesta kryptovaluuttalompakon siemenlauseesta, mikä sisältää 12 erilaista sanaa.

AUNT	DOG	SON	BIKE
BOAT	DAD	WOLF	CAR
SHEEP	MOM	PLANE	CAT

Kuva 5. kryptovaluuttalompakon siemenlauseet

3.1.2 Kylmät lompakot

Kylmälompakko voi tarkoittaa ulkoista laitetta, mihin yksityisen avaimen voi tallentaa. Nano Ledger on yksi tunnetuimmista kylmälompakkolaitemerkeistä. Kylmälompakkolaitteiden avulla voidaan hallita kryptovaluuttoja liittämällä ne tietokoneeseen sekä lataamalla tarvittava ohjelmisto koneelle. Usein laitelompakot muistuttavat ulkoisilta muodoiltaan muistitikkua, mutta ne voivat olla myös esimerkiksi luottokortin näköisiä. On huomattavaa, että myös kylmälompakkolaitteiden yhteydessä yksityiset avaimet voidaan palauttaa siemenlauseiden avulla. (Hyppönen 2023b.) Kylmälompakkolaitteet on yleensä salattuja ja salasanalla suojattuja laitteita. Kylmänä lompakkona pidetään myös tapaa, missä yksityinen avain kaiverretaan metallilevyyn tai kirjoitetaan paperille ylös.

Yksityinen avain on siis keskiössä kryptovaluutan hallinnassa, koska lohkoketjuihin merkitään muuttumattomasti tiedot siitä, mikä julkinen/yksityinen avainpari hallitsee mitäkin osaa kryptovaluutasta ja vain yksityisen avaimen avulla näiden varojen liikuttaminen on mahdollista.

3.2 Kryptovaluutan muuttaminen perinteiseksi rahaksi

Jotta kryptovaluuttaa pystyy muutamaan perinteiseksi rahaksi, vaaditaan väliin toimija, joka on halukas tekemään muutoksen. Helpoiten edellä mainittu tapahtuu kryptovaluuttoja välittävissä keskitetyissä pörsseissä, jolloin kryptovaluutta vaihdetaan perinteiseksi rahaksi voimassa olevien kurssien mukaan. Kryptovaluuttoja välittävissä keskitetyissä pörsseissä on jopa omia pankkikortteja, joihin voi siirtää rahaa myymällä ensin kyseisessä pörssissä kryptovaluuttaa ja siirtämällä sen sitten kyseisen pörssin pankkikortille. Tällöin toimenpide on nopea. Lisäksi on olemassa automaatteja, joiden kautta bitcoinia pystyy muuttamaan käteiseksi rahaksi. (Bitpay 2023.)

3.3 Kryptovaluuttojen hankkiminen

Kryptovaluuttoja pystyy hankkimaan työtodennusmallissa louhimalla. Kryptovaluuttoja voi myös hankkia julkaisemalla oman kryptovaluutan tai tokenin. Mikäli henkilöllä on jo hallussaan kryptovaluuttaa, pystyy hän asettamaan sen panokseksi panokseen perustuvassa todentamismallissa ja ansaitsemaan siten itselleen lisää kryptovaluuttaa. Yleensä kryptovaluuttaa hankitaan kuitenkin ostamalla sitä. Ostaminen tapahtuu yleensä keskitetyn tai hajautetun pörssin kautta. Toki on myös mahdollista, että joku, jolla on jo hallussaan kryptovaluuttaa lähettää sitä toiselle henkilölle.

3.3.1 Keskitetyt pörssit

Keskitetyt pörssit toimivat perinteisen kauppapaikan tapaan. Tällöin käyttäjät menevät normaaliin tapaan kyseisen pörssin nettisivuille, missä he luovat tunnukset pörssiin. Pörssissä käyttäjät voivat ostaa kryptovaluuttoja siirtämällä perinteistä rahaa pörssiin tai siirtämällä pörssiin jo aiemmin

hallussaan olevaa kryptovaluuttaa. Keskitettyjen pörssien taustalla oleva yritys hallitsee käyttäjän kryptovaluuttoja ja niiden yksityisiä avaimia. Näin ollen keskitettyjen pörssien toimintaa voi verrata perinteisten pankkien ja rahoituslaitosten toimintaan. Tällöin käyttäjä luovuttaa omaisuutensa hallinnan kolmannen osapuolen käsiin. Hyvänä puolena on, ettei käyttäjän tällöin tarvitse itse huolehtia kryptovaluuttojen yksityisistä avaimista. (Reiff 2021.) Tunnettuja keskitettyjä kryptovaluuttapörssejä ovat mm. Binance ja Coinbase. Suomalaisista kryptovaluuttapörsseistä tunnetuin lienee Coinmotion niminen pörssi. Useimmat keskitetyt pörssit vaativat käyttäjiä todentamaan henkilöllisyytensä tilin luonnin yhteydessä esimerkiksi passien avulla.

3.3.2 Hajautetut pörssit

Hajautetussa pörssissä kauppa suoritetaan älysopimusten avulla, eikä kaupankäyntiin liity älysopimusten lisäksi kolmatta osapuolta. Tällaista kaupankäynnistä puhuttaessa käytetään termiä automated market maker (AMM). Tällöin käyttäjät hyödyntävät kryptovaluuttalompakossaan olevia varoja käydessään kauppaa. Hajautetun pörssin alaisuuteen on luotu kuvainnollisesti älysopimusten avulla valuuttaparisammiota, mitkä sisältävät kryptovaluuttaa. Hajautetut pörssit houkuttelevat sijoittajia tarjoamaan likviditeettiä älysopimukseen antamalla osan kaupankäyntiin määritellystä siirtomaksusta likviditeetin tarjoajalle. Tällöin likviditeetin tarjoaja lukitsee hallussaan olevaa kryptovaluuttaa älysopimuksen alaisuuteen ja mikäli joku haluaa ostaa tuota kryptovaluuttaa itselleen, laukaisee hän älysopimuksen, mikä määrittelee hinnan ostokselle. Hinta sisältää siirtomaksun, josta osa ohjautuu likviditeetin tarjoajalle ja vaihdossa likviditeetin tarjoaja saa ostajan vaihdossa käyttämän kryptovaluutan itselleen. (Chainlink 2023.) Tunnetuin hajautettu pörssi lienee Uniswap mikä toimii ethereum-kryptovaluutan päällä.

3.3.3 Pörsseihin liittyvä rikollisuus

On olemassa lukuisia esimerkkejä siitä, että keskitetyn pörssin toimijat ovat väärinkäyttäneet niiden käyttäjien varoja, aiheuttaen valtavia tappioita asiakkailleen. Tuoreimpana esimerkkinä FTX nimisen keskitetyn kryptovaluuttapörssin kaatuminen (Jeans & Emerson 2022). Useat keskitetyt kryptovaluuttapörssit ovat myös joutuneet eri viranomaisten hampaiseen mm. rahanpesuepäilyjen sekä sanktioitujen tahojen siirtojen välittämisen vuoksi. Esimerkkinä vuoden 2023 poliisioperaatio, minkä yhteydessä FBI ja Ukrainan valtiolliset toimijat sulkivat yhdeksään kryptovaluuttapörssiin liittyneet nettiosoitteet sekä takavarikoivat niihin liittyviä palvelimia. Kyseisten pörssien kautta epäiltiin liikutellun erilaisiin rikoksiin liittyvää varallisuutta, ja kyseisillä pörsseillä oli puutteita niiden käyttäjien todentamisessa, mikä mahdollisti rikollisen toiminnan (United States Attorney's Office Eastern District of Michigan 2023). Myös hyvin tunnettu keskitetty kryptovaluuttapörssi Binance on ollut Yhdysvaltojen viranomaisten tutkinnan kohteena. Vuonna 2023 Yhdysvaltain viranomaiset tutkivat, onko Binancen kautta sallittu sanktioitujen venäläisten tahojen rahaliikennettä. (Andersen 2023.)

3.3.4 Airdrop

Kryptovaluutat mainostavat itseään airdroppien avulla. Käyttäjiä voidaan esimerkiksi kannustaa hankkimaan jotain kryptovaluuttaa siten, että hankkimalla kyseistä kryptovaluuttaa ja pitämällä sitä kryptovaluuttalompakossaan tiettynä ajankohta, kyseiseen lompakkoon lähetetään jokin määrä samaa kryptovaluuttaa ilmaiseksi. Tällä pyritään lisäämään kyseisen kryptovaluutan tunnettavuutta ja käyttöä. (Binance 2023b.)

3.3.5 Sovelluksen käyttö

On olemassa sovelluksia, joita käyttämällä voi tienata kryptovaluuttaa. Esimerkiksi Brave niminen nettiselain jakaa mainostajilta saatuja maksuja selaimen käyttäjille bat-kryptovaluuttana, mikäli nämä katsovat mainoksia selaimessaan (Brave 2023).

4 Fyysisen takavarikoinnin mahdollistava lainsäädäntö

Tutkimuksessa ei tutkittu sitä, kuinka kryptovaluuttoihin liittyvää rikostutkintaa tulisi suorittaa, eikä tutkimuksen tarkoituksena ole toimia ohjeena kryptovaluuttoihin liittyvässä rikostutkinnassa. Tutkimuksessa ei myöskään käydä läpi kryptovaluuttoihin liittyviä taktisen rikostutkinnan menetelmiä. Tutkimuksen tulosten, pohdinnan ja ymmärrettävyyden vuoksi tutkimuksessa käydään kuitenkin läpi keskeistä lainsäädäntöä siltä osin, mikä on oleellista kryptovaluuttojen fyysisen löytämisen suhteen massarikosten tutkinnan yhteydessä. Tutkimuksesta on rajattu pois salaisten pakkokeinojen tarkastelu, koska ne muodostavat hyvin pienen osan massarikosten yhteydessä käytettävistä pakkokeinoista. Salaisten pakkokeinojen osalta rajaus on tehty myös niiden laajuuden vuoksi. Tutkimuksesta on rajattu pois myös erilaisiin tietopyyntöihin liittyvien toimenpiteiden ja lainsäädännön tarkastelu niiden laajuuden vuoksi, vaikka niitä käytetään merkittävissä määrin myös massarikosten tutkinnan yhteydessä.

Poliisitoiminta on sidottu lainsäädäntöön. Tärkeimmät lait joihin poliisitoiminta pohjautuu ovat perustuslaki, poliisilaki, esitutkintalaki, pakkokeinolaki sekä rikoslaki. Poliisin toimintakenttä on kuitenkin laaja, minkä vuoksi poliisin työssä joudutaan välillä tekemisiin miltei kaikkien lakien kanssa.

4.1 Takavarikko

Pakkokeinolain (22.7.2011/806) 7 luvun 1 §:ssä määritellään takavarikoinnista tiivistetysti seuraavaa. Esine, data tms. saadaan takavarikoida, mikäli sitä voidaan käyttää todisteena rikosasiassa, se on joltakulta viety tai se voidaan tuomita menetetyksi. Kyseisessä pykälässä määritellään siis se, milloin jokin asia voidaan ottaa viranomaisten haltuun rikosprosessin aikana. Käytännössä poliisi voi takavarikoida esimerkiksi huumeita, rikoksen tekovälineen, kryptovaluuttoja tai vaikkapa matkapuhelimen, mikä pitää sisällään kryptovaluuttalompakkosovelluksen, mikäli ne liittyvät tutkittavaan rikokseen.

Pakkokeinolain 7 luvun 7 §:ssä todetaan tiivistetysti, että takavarikoinnista tai esineen jäljentämisestä päättää pidättämiseen oikeutettu virkamies, mikä on käytännössä tutkinnanjohtaja. Tutkinnanjohtajina toimivat yleensä komisarion virkaa hoitavat virkamiehet. Pakkokeinolain 7 luvun 8 §:ssä todetaan tiivistetysti poliisimiehen olevan oikeutettu ottamaan takavarikoitava esine haltuunsa, mutta hänen on viivytyksettä ilmoitettava haltuunotosta pidättämiseen oikeutetulle virkamiehelle, jonka on tehtävä viivytyksettä päätös mahdollisesta esineen takavarikoinnista tai jäljentämisestä.

4.2 Vakuustakavarikko

Vakuustakavarikosta säädetään pakkokeinolain 6 luvun 1§:ssä seuraavaa.

> Omaisuutta saadaan määrätä vakuustakavarikkoon sakon, rikokseen perustuvan vahingonkorvauksen tai hyvityksen taikka valtiolle menetettäväksi tuomittavan rahamäärän maksamisen turvaamiseksi. Edellytyksenä vakuustakavarikon määräämiselle on, että omaisuus kuuluu henkilölle, jota on syytä epäillä rikoksesta tai joka voidaan rikoksen johdosta tuomita korvaamaan vahinko tai maksamaan hyvitystä taikka menettämään valtiolle rahamäärä, ja on olemassa vaara, että mainittu henkilö pyrkii välttämään sakon, vahingonkorvauksen, hyvityksen tai rahamäärän maksamista kätkemällä tai hävittämällä omaisuuttaan, pakenemalla tai muulla näihin rinnastettavalla tavalla. Vakuustakavarikkoon saadaan panna omaisuutta enintään määrä, jonka voidaan olettaa vastaavan tuomittavaa sakkoa, vahingonkorvausta, hyvitystä tai menettämisseuraamusta.

Pakkokeinolain 6 luvun 2§:ssä säädetään tiivistetysti, että vakuustakavarikosta päättää tuomioistuin. Pakkokeinolain 6 luvun 3§:ssä taas säädetään tiivistetysti, että mikäli asia ei siedä viivytystä, voi pidättämiseen oikeutettu virkamies päättää väliaikaisesta vakuustakavarikosta, mikä pitää viedä tuomioistuimen päätettäväksi viikon sisällä tai muutoin vakuustakavarikko päättyy.

Pakkokeinolain 6 luvun 11§:ssä säädetään tiivistetysti, että vakuustakavarikkoa koskevasta vahingonkorvausvastuusta ja kulujen korvaamisessa noudatetaan oikeudenkäymiskaaren 7 luvun 11 §:ää.

Oikeudenkäymiskaaren (1.1.1734/4) 7 luvun 11§ määrittelee seuraavaa. ” Hakijan, joka on tarpeettomasti hankkinut turvaamistoimen, on korvattava vastapuolelle turvaamistoimesta ja sen täytäntöönpanosta aiheutunut vahinko ja asiassa aiheutuneet kulut.”

Mikäli kryptovaluutat pystytään takavarikoimaan rikokseen liittyen, on menettely lain suhteen selkeää. Vakuustakavarikoiden osalta tilanne on hieman toinen. Tutkimuksen tekijän oman kokemuksen mukaan vakuustakavarikoiden käytöllä on suhteellisen korkea käyttökynnys, ainakin lievempien rikosten tutkinnan yhteydessä. Uskon suurimman syyn tähän löytyvän siitä, että mikäli esitutkinnan yhteydessä on käytetty vakuustakavarikointia ja myöhemmin rikoksesta epäilty vapautetaan syytteistä, määrätään valtio yleensä maksamaan korvauksia epäilylle. Korvauksia joudutaan yleensä maksamaan, vaikka vakuustakavarikolle olisi rikostutkinnan aikana ollut vahvat ja perustellut syyt. (Korkein oikeus 2022.)

4.3 Koti- ja paikkaetsintä

Pakkokeinolain luvussa 8 määritellään etsinnästä.

Pakkokeinolain 8 luku 1 § määrittelee koti ja paikkaetsinnän edellytykset. Tiivistetysti koti ja paikkaetsintä voidaan pakkokeinolain mukaan suorittaa, mikäli epäillystä rikoksesta säädetty ankarin rangaistus on vähintään 6 kk. vankeutta ja etsinnän avulla voidaan olettaa löytyvän mm. rikokseen liittyvää tietoa, tavaraa tai vakuustakavarikoitavaa omaisuutta. Eli etsintä voidaan suorittaa jo melko lievien rikosten tutkinnan yhteydessä. Kotietsintä on jaettu kahteen osaan eli yleiseen ja erityiseen. Yleinen kotietsintä kohdistuu paikaan mikä rikoslain mukaan nauttii kotirauhan suojaa esim.

epäillyn käytössä oleva asunto. Erityinen kotietsintä taas kohdentuu paikaan missä oletetaan säilytettävän esim. potilassalaisuuteen liittyvää materiaalia. Tarkemmat määritelmät erityiseen kotietsintään löytyvät oikeudenkäymiskaaren (1.1.1734/4) 17 luvusta. Paikkaetsintä taas kohdistuu esim. ajoneuvoon tai liikekiinteistöön. Koti- ja paikkaetsinnästä päättää pidättämiseen oikeutettu virkamies mutta poliisimies voi suorittaa koti- ja paikkaetsinnän myös ilman päätöstä, mikäli asia ei siedä viivytystä.

4.4 Henkilötarkastus

Pakkokeinolain 2 luvun 1§:ssä määritellään poliisimiehen kiinniotto-oikeudesta, minkä mukaan poliisi saa ottaa henkilön kiinni rikoksen selvittämistä varten, mikäli rikos on veres tai epäilty pakenee. Lisäksi poliisimies saa ottaa kiinni epäillyn, joka on pidätettävä tai vangittava tai kenet tuomioistuin on määrännyt kiinniotettavaksi. Lisäksi poliisimies saa ottaa kiinni henkilön ilman pidätysmääräystä, jos pidättäminen voi muutoin vaarantua. Tällöin kiinniottamisesta on ilmoitettava välittömästi pidättämiseen oikeutetulle virkamiehelle, jonka on päätettävä pidätyksestä 24 tunnin sisällä kiinniotosta. Yli 12 tunnin kiinnipitäminen edellyttää pidättämisen edellytysten olemassaoloa.

Henkilötarkastuksesta säädetään pakkokeinolain 8 luvun 3§:ssä, missä todetaan, että henkilötarkastus voidaan suorittaa, mikäli pakkokeinolain 8 luvun 2§:n 1mom. 2 kohdan ehdot täyttyvät. Poliisilaissa määritellään erikseen henkilölle tehtävästä turvallisuustarkastuksesta ja poliisilakiin perustuvista kiinniotoista. Henkilö tarkastus voidaan tehdä, mikäli henkilön epäillään syyllistyneen rikokseen, mistä säädetty ankarin rangaistus on vähintään 6 kk. vankeutta tai kyseessä on lievä pahoinpitely, näpistys, lievä kavallus, lievä luvaton käyttö, lievä moottorikulkuneuvon käyttövarkaus, murtovälineen hallussapito, lievä alkoholirikos, liveä vahingonteko tai lievä petos. Muu kuin rikoksesta epäilty saadaan tarkastaa vain, jos on erittäin pätevä syy epäillä, että hänen hallustaan löytyy takavarikoinnin edellytysten täyttävä asia.

4.5 Laite-etsintä

Pakkokeinolain 8 luvun 21§ määrittää laite-etsinnän edellytykset. Laite-etsinnällä tarkoitetaan yleensä tietoteknisen laitteen tutkimista tai sen tietosisällön jäljentämistä. Laite-etsintä saadaan suorittaa epäillyn laitteisiin, mikäli henkilön epäillään syyllistyneen rikokseen, minkä ankarin rangaistus on vähintään puoli vuotta vankeutta tai asiaan liittyy yhteisösakon antamiseen. Laite-etsinnän edellytykset ovat samat kuin takavarikoinnissa. Laite-etsintä voidaan toimittaa myös laitteen palauttamiseksi siihen oikeutetulle, jos on syytä olettaa, että se on rikoksella joltakulta viety.

5 Kryptovaluuttojen yksityisyys ja kryptovaluuttoihin liittyvä rikollisuus

Kryptovaluutat ovat yleensä puolittain anonyymejä. Tällä tarkoitetaan sitä, että mikäli kryptovaluutan käyttämä lohkoketju on julkinen, pystyy kuka tahansa tarkastelemaan lohkoketjun sisältämiä tietoja. Lohkoketjuun tallennetaan kaikki siirrot sekä se, kuinka paljon kunkin julkisen/yksityisen avainparin hallinnassa on kryptovaluuttoja. Näin ollen, mikäli jonkin tahon julkinen osoite saadaan selville, pystytään lohkoketjua tarkastelemalla selvittämään kyseisen osoitteen aktiviteetit. Lohkoketjusta pystytään selvittämään mistä tarkasteltavaan osoitteeseen on siirretty kryptovaluuttaa ja mihin siitä on lähetetty kryptovaluuttaa. Kryptovaluutat ovat kuitenkin ns. ohjelmoitavaa rahaa ja niihin liittyviä siirtoja pystyy helposti ketjuttamaan, jolloin siirtojen jäljittäminen ei ole helppoa. Siirtojen analysointiin on kuitenkin kehitetty erilaisia analyysiohjelmistoja. Kryptovaluuttoihin liittyvien jäljitysmenetelmien tarkempi tarkastelu on rajattu tutkimuksesta pois niiden laajuuden vuoksi.

Kryptovaluuttoihin liittyen on olemassa palveluilta, joiden avulla kryptovaluuttojen alkuperää pyritään hävittämään. Tällöin siirrot voidaan ohjata palveluun, missä ne sekoitetaan muihin siirtoihin, jolloin siirtojen jäljittäminen on haastavampaa. (Hendrickson & William 2022, s 202.) Yksi tällainen palvelu on Tornado Cash niminen älysopimus, mikä toimi alun perin Ethereum-kryptovaluutan päällä, mistä se on laajentunut myös useiden muiden protokollien käyttöön. Palvelun käyttäjä tallentaa älysopimukseen kryptovaluuttaa. Talletussummien määrä on ennalta määrätty tiettyihin kokoihin. Tallennuksen yhteydessä käyttäjä saa merkkisarjan sisältävän tiedoston, mikä toimii eräänlaisena yksityisenä avaimena ja sen avulla kryptovaluuttaa pystyy myöhemmin nostamaan Tornado Cashin älysopimuksesta. Tämän jälkeen Tornado Cashin käyttäjä luo uuden kryptovaluuttalompakon ja odottaa riittävän pitkän aikaa, jotta myös muut tahot tekevät talletuksia älysopimukseen, jotta talletettu summa pystyy sekoittumaan muihin talletuksiin. Myöhemmin Tornado Cashin käyttäjä nostaa tallentamansa kryptovaluutan älysopimuksesta uuteen kryptovaluuttalompakkoon alussa saamansa tiedoston avulla. Koska alkuperäinen talletus on sekoittunut muihin älysopimukseen tehtyihin talletuksiin, katkeaa kryptovaluutan alkuperä kyseiseen palveluun. Tornado Cash käyttää toiminnassaan hyväksi ns. zero knowledge proof konseptia. (The Blockchain Guy 22.2.2022.) Zero knowledge proof-konseptin tarkempi käsittely on rajattu tutkimuksesta pois sen laajuuden vuoksi.

Yhdysvaltojen valtionvarainministeriö asetti Tornado Cashin sanktiolistalleen vuonna 2022. Sanktiolistalle asetetaan tahoja, joiden koetaan muodostavan uhan Yhdysvaltojen turvallisuudelle ja sanktiolistalle joutuvia tahoja kohtaan asetetaan voimakkaita pakotteita sekä ehtoja eli käytännössä niiden toiminta kielletään Yhdysvalloissa. Yhdysvaltojen valtionvarainministeriön mukaan Tornado Cashin kautta on vuoden 2019 jälkeeni pesty rahaa yli 7 miljardin dollarin edestä. Vaikka Yhdysvaltojen valtionvarainministeriön mukaan suurin osa kryptovaluuttojen käytöstä on laillista,

voidaan niitä käyttää kuitenkin myös rikolliseen toimintaan mm. hajautettujen kryptovaluuttapörssien ja sekoituspalveluiden kautta. Lisäksi kryptovaluuttoja käytetään maksuna pimeän verkon markkinapaikoilla. Valtionvarainministeriön mukaan kryptovaluuttoja käytetään hyväksi myös tietoverkossa tapahtuvissa rikoksissa, kuten ns. ransomware eli lunnasvaatimuksiin perustuvissa rikoksissa. (Us. Department of the Treasury 2022.) Ransomware-rikoksissa toimintatapana on usein se, että rikoksen uhrin tietokoneelle ujutetaan haittaohjelma minkä avulla esimerkiksi salataan uhrin tietokoneen tiedot. Salaamisen jälkeen uhrille ilmoitetaan, että hänen täytyy maksaa kryptovaluuttaa kiristäjille, jotta he luovuttavat uhrille avaimen, minkä avulla salauksen voi poistaa.

Chainanalysin vuonna 2023 tekemän tutkimuksen mukaan laittomaan toimintaan liittyviin kryptovaluuttaosoitteisiin kytkeytynyt arvonsiirto on ollut kasvussa. Vuonna 2017 näiden siirtojen arvo oli alle 5 miljardia dollaria, kun vuonna 2022 siirtojen arvo ylitti jo 20 miljardin dollarin rajan. Vuoden 2022 laittomaan toimintaan kytkeytyneiden siirtojen arvosta noin 43 % koski siirtoja sanktioituihin osoitteisiin ja nämä siirrot muodostivat suurimman osan laittomasta toiminnasta. Toiseksi suurimman osuuden muodostivat huijauksiin liittyneet siirrot ja kolmanneksi suurimman osan muodostivat varastettuihin varoihin liittyneet siirrot. Laittomaan toimintaan liittyvä kryptovaluuttaliikenne muodosti vuonna 2022 noin 0,24% osan kaikesta kryptovaluuttaliikenteestä. (Chainanalysis 2023, 4-7.)

Yhdysvaltojen valtionvarainministeriö on asettanut kasvavissa määrin kryptovaluuttoihin liittyviä tahoja ja osoitteita sanktiolistalleen. Vuonna 2021 sanktiolistalla oli noin 100 kryptovaluuttaosoitetta mutta vuonna 2022 määrä oli kohonnut jo noin 300 osoitteeseen. (Chainanalysis 2023, 10-11.) Sanktioiden vaikutus on ollut vaihteleva. Esimerkiksi Tornado Cashin käyttö laski voimakkaasti sen jouduttua sanktiolistalle, mutta toisen kryptovaluuttapalvelun eli Garantex-kryptovaluuttapörssin käyttö on vain kasvanut sanktiolistalle joutumisen jälkeen. (Chainanalysis 2023, 18.)

Sekoituspalveluiden lisäksi on myös olemassa yksityisyyteen tähtääviä kryptovaluutta protokollia, jotka pyrkivät peittämään siirtoja. Yksi tunnetuimmista yksityisyyteen tähtäävistä protokollista on Monero niminen kryptovaluutta. (Hendrickson & Luther 2022, 202.)

Käteisellä rahalla on merkittävä rooli rikollisen toiminnan arvonsiirrossa. On jopa esitetty näkemyksiä, joiden mukaan rikollisen toiminnan ja veronkierron minimoimiseksi käteisestä rahasta tulisi luopua tai ainakin sen käyttöä tulisi vähentää. Tähän mennessä valtiot ovat tehneet varsin maltillisesti toimenpiteitä käteisestä rahasta luopumisen suhteen, Ruotsin ollessa kuitenkin pisimillä tässä kehityskulussa. Myös Euroopan unioni on tehnyt asiaan liittyen toimenpiteitä esimerkiksi lopettamalla 500 euron seteleiden tuottamisen. On kuitenkin todettu, että liiallinen käteisen käytön vähentäminen siirtää rikollisen toiminnan arvonsiirtoa kohti muita vaihtoehtoja kuten esimerkiksi kryptovaluuttoja. (Hendrickson & Luther 2022, .200-207.)

Vaikka erilaiset digitaaliset maksutavat ovat kehittyneet huimaa vauhtia, monissa maissa käytetään kuitenkin yhä nykyisinkin huomattavan paljon käteistä rahaa. Vaikka käteinen raha on helppoa hukata eikä se kasva korkoa, liittyy käteisen rahan käyttöön kuitenkin useita hyötyjä. Käteistä rahaa käytettäessä ei tarvita pankkitilejä tai internettiä ja näin käteisen rahan käyttö tarjoaa hyvää yksityisyydensuojaa. Käteisen rahan käyttöön ei myöskään pysty puuttumaan, ellei varoja fyysisesti takavarikoida. (Hendrickson & Luther 2022, .200-207.)

Ainoa selkeä puute käteisen rahan käytössä yksityisyyttä ajateltaessa on siihen todennäköisesti sisältyvä fyysisen tapaamisen tarve arvonsiirron yhteydessä. Fyysinen tapaaminen heikentää käteisen rahan käytön yksityisyyden suojaa. Kryptovaluutat poistavat käteisen rahan arvonsiirtoon liittyvän vaiheen, missä arvonvaihtajien täytyy tavata toisensa. Toisaalta kryptovaluutan arvonsiirrot jättävät pysyvän merkinnän lohkoketjuihin, mitkä ovat julkisia. Parantaakseen yksityisyyden suojaa kryptovaluuttojen käyttäjät voivat käyttää protokollia tai palveluita, joissa yksityisyys on otettu paremmin huomioon tai joiden avulla pystytään kätkemään tai sekoittamaan siirtoja. Edellä mainitun perusteella voidaan tehdä yhteenveto, minkä mukaan jotkin kryptovaluutat ja niihin liittyvät palvelut pystyvät tarjoavat paremman yksityisyydensuojan kuin käteinen raha. (Hendrickson & Luther 2022, .200-207.)

Europolin raportin mukaan kryptovaluuttojen käyttö rikollisessa toiminnassa on kasvanut, mutta ilmiö muodostaa edelleen hyvin pienen osan rikoksiin liittyvästä arvonsiirrosta ja sen todellista kokoa on hankalaa arvioida. Kryptovaluuttoja on kuitenkin käytetty rahanpesuun ja sen käyttötavat ovat muuttuneet mutkikkaammiksi selvittää. Kryptovaluuttaa on alettu käyttää kasvavissa määrin rikollisen toiminnan maksutapana ja rikoksella hankittua rahaa on sijoitettu kryptovaluuttoihin. Kryptovaluuttaa ei enää käytetä pelkästään tietoverkoissa tapahtuviin rikoksiin vaan sen käyttö on lisääntynyt myös perinteisten rikosten yhteydessä, missä arvoa täytyy siirtää henkilöltä toiselle. Kryptovaluutoilla ostetaan myös luvattomia tuotteita ja materiaalia. Yleisimmin kryptovaluuttoja on havaittu käytettävän petosten yhteydessä. Tietoverkkorikoksissa kryptovaluutat liittyvät kiinteältä osin ns. ransomware tapauksiin. Raportissa mainittiin, että kryptovaluuttaa ei juurikaan käytetä terrorismin rahoitusmuotona. Kryptovaluuttoihin liittyvän lainsäädännön kehitys on raportin mukaan merkinnyt sitä, että kryptovaluuttojen käyttäjistä kerätään entistä enemmän yksilöivää tietoa, mikä osaltaan auttaa kryptovaluuttojen jäljityksessä. Raportissa todetaan kryptovaluuttoihin liittyvän rikollisen aktiivisuuden muodostavan kuitenkin varsin pienen osuuden kryptovaluuttojen ekosysteemissä ja rikollisuus näkyy paljon vahvemmin perinteisen finanssitalouden piirissä. (Euripol 2021.)

Suomen mediassa on uutisoitu lukuisista rikoksista, mitkä liittyvät kryptovaluuttoihin. Vuonna 2020 poliisi kertoi Bitcoinin liittyneen kiinteällä tavalla tor-verkon Silkkitie markkinapaikalla käytyyn huumausainekauppaan. Silkkitie toimi vuodesta 2013 lähtien, kunnes tulli takavarikoi sen

verkkopalvelimen vuonna 2019.(Poliisi 2020.) Vuonna 2018 taas uutisoitiin, kuinka rattijuopon pidätys johti laajaan huumausainerikostutkintaan, minkä yhteydessä poliisi takavarikoi yli 700 000 euron arvosta bitcoineja. Tietämättä kyseisen asian taustoja, tapaus osoittaa hyvin, kuinka massarikosten tutkinnan yhteydessä voidaan päästä ns. isojenkin juttujen jäljille, seuraamalla arvonsiirtoja eli tässä tapauksessa kryptovaluuttojen liikkeitä. (Välimaa 2018.) Vuonna 2021 Helsingin poliisista kommentoitiin Ilta-Sanomille kryptovaluuttoihin perustuvien huijausten lisääntyneen, vaikka ne muodostivat yhä pienen osan tutkituista talousrikoksista. Tuolloin tapeteilla olivat tapaukset, joissa sijoittajia houkuteltiin sijoittamaan rahojaan kryptovaluuttoihin liittyviin sijoituskohteisiin, mitkä osoittautuivatkin puhtaiksi huijauksiksi. (Linnake 2021.)

Se mihin suuntaan kryptovaluuttojen ja rikollisuuden suhde tulevaisuudessa kehittyy, on vielä hämärän peitossa. Johtopäätösten tekeminen on hankalaa koska pelkästään se, tuleeko kryptovaluutoista laajasti ja helposti käytettäviä arvonsiirtomenetelmiä on epäselvää. (Trozze ym. 2022, 11-12.) Se mitenkä rikolliset tulevaisuudessa hyödyntävät esimerkiksi metaversea ja keinoälyä on mielenkiintoinen asia pohdittavaksi. Metaverse tarkoittaa virtuaalitodellisuutta tai pikemminkin reaalimaailman jatketta, missä sen käyttäjät voivat toimia hyvin pitkälle samalla tavalla kuin reaalimaailmassakin (Bosworth & Clegg 2021). Osa metaverseista toimii siten, että niistä käyttäjät pystyvät ostamaan esimerkiksi virtuaalimaata sekä erilaisia esineitä, samaan tapaan kuin reaalimaailmassakin. Yksi tällainen metaverse on nimeltään Decentraland ja se linkittyy vahvasti Ethereum-kryptovaluuttaan. (Cointelegraph s.a.) Parin viime vuoden aikana ajatus metaverseista onkin ollut vahva narratiivi kryptovaluuttojen yhteydessä. Mikäli metaverset saavuttavat tulevaisuudessa suurempaa suosiota, etsiytyvät myös rikolliset niihin kasvavissa määrin, mikä voi tuoda yllättäviä ilmiöitä esiin.

Tulevaisuuden näkymät kryptovaluuttoihin liittyvän rikollisuuden suhteen ovat siis vielä hämärän peitossa. Lienee kuitenkin selvää, että mikäli kryptovaluuttoihin liittyvää rikollisuutta halutaan tulevaisuudessa suitsia, täytyy asiaan liittyvien tahojen, kuten esimerkiksi kryptovaluuttapörssien olla avoimempia ja niiden täytyy tehdä kasvavissa määrin yhteistyötä viranomaisten kanssa. (Trozze ym. 2022, 11-12.)

Kryptovaluutat tarjoavat monia isoja etuja, kun niitä verrataan perinteiseen talousjärjestelmään. Kryptovaluuttojen kautta on mahdollista siirtää arvoa maailmanlaajuisesti huomattavasti nopeammin kuin ennen. Kryptovaluuttojen avulla voidaan tuottaa palveluita, joita ei ennen ole pystytty tuottamaan. Esimerkkinä voisi toimia vaikkapa erilaisten asioiden tokenisointi. Kryptovaluuttoihin liittyviä etuja ja uusia käyttömuotoja voi kehitellä, vaikka kuinka paljon, mutta niiden toimivuus tarvitsee perustaksi myös jonkinlaista toimivaa lainsäädäntöä. Tällä hetkellä kryptovaluuttojen käyttäjät ovat

pitkälti oman onnensa varassa, mikä toisaalta on myös kryptovaluuttojen syvin ydin eli ne on kehitetty käyttäjien hallinnoitaviksi.

Kryptovaluuttojen käyttämiseen ja niiden hallinnointiin liittyvää lainsäädäntöä kehitteillä useissa valtioissa ympäri maailmaa. Kryptovaluuttojen sääteleminen lakien avulla on kuitenkin haastavaa niiden toimintamekanismien vuoksi ja yhteiset kansainväliset linjaukset lakien suhteen puuttuvat vielä. (George 2023.)

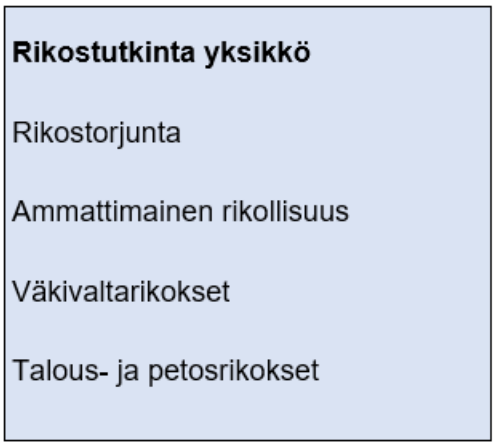
6 Tutkimuksen kohde, haastattelun tulokset ja johtopäätökset

6.1 Helsingin poliisilaitos

Helsingin poliisilaitos on perustettu vuonna 1826 ja se on Suomen suurin poliisilaitos. Laitoksella työskentelee noin 1600 henkilöä. Poliiseja työntekijöistä on noin 1300. (poliisi s.a b.) Helsingin poliisilaitoksen aluealla asuu noin 660 tuhatta ihmistä (Wikipedia s.a).

Koronavuonna 2021 Helsingin poliisin tietoon tuli tilastokeskuksen mukaan rikoslaki rikoksia yhteensä 73 426 kappaletta eli laskennallisesti noin 200 tapausta päivässä (Tilastokeskus 2022).

Helsingin poliisilaitoksen rikostorjuntayksikkö on yksi neljästä Helsingin poliisilaitoksen rikoksia tutkivista sektoreista. Kyseisen yksikön sisällä on vielä jakoa tutkittavien rikosten ominaisuuksien suhteen, mutta tutkimukseen valittiin yksikön osa, mikä tutkii ns. massarikoksia. Lähtökohtaisesti kyseisen yksikön tutkimissa jutuissa rikos on jo tapahtunut ja on olemassa jokin tekijä, minkä kautta rikoksentekijä on mahdollista löytää käytettävissä olevien resurssien puitteissa. Alla kaavio Helsingin poliisilaitoksen rikostutkintayksikön rakenteesta. Rikostutkintayksikkö koostuu neljästä sektorista mitkä ovat rikostorjunta, ammattimainen rikollisuus, väkivaltarikokset ja talous- ja petosrikokset.



Kuva 7. Helsingin poliisilaitoksen rikostutkinnan organisaatiokaavio.

Tutkimuksen tekemisen hetkellä tutkittavan yksikön työntekijämäärä oli noin 50-60 henkilöä. Yksikössä työskenteli rikosylikonstaapeleja, vanhempia rikoskonstaapeleja sekä tutkintasihteereitä. Yksikössä oli myös säännöllisesti kierrolla kenttätöistä vanhempia konstaapeleja ja poliisikoulutuksen liittyvien työharjoitteluiden kautta nuorempia konstaapeleja. Rikosylikonstaapelit vastasivat tutkintaryhmien päivittäisestä johtamisesta ja henkilöstöhallinnosta, minkä lisäksi he suuntasivat tutkintaa sekä ns. seuloivat eli luokittelivat ja priorisoivat tutkittavia rikoksia. Vanhemmat rikoskonstaapelit ja vanhemmat konstaapelit hoitivat rikosten tutkintaa pitkälle omatoimisesti, kuitenkin pakkokeinoja

käytettäessä heidän täytyi pyytää luvat pakkokeinojen käytölle tutkinnanjohtajilta, jotka myös linjasivat, miten tutkinnoissa edetään yhdessä rikosylikonstaapelien kanssa. Tutkimuksen tekohetkellä ryhmien ulkopuolella olleet rikoskomisariot toimivat tutkinnanjohtajina, vastaten asiantuntijoina pakkokeinojen käytöstä sekä rikostutkinnan laadusta ja oikeellisuudesta. Nuoremmat konstaapelit hoitivat rikostutkintaa vanhempien rikoskonstaapeleiden sekä vanhempien konstaapeleiden valvonnassa. Tutkintasihteerit hoitivat tutkintaa liittyviä käytännön asioita, kuten tietopyyntöjä ja avustivat monella tapaa rikostutkijoita heidän työssään.

6.2 Tutkimuksen haastattelu osion tausta

Tutkimukseen liittyvä kysely suoritettiin Helsingin poliisilaitoksella loppuvuodesta 2022. Kysely koostui yhteensä 20 kysymyksestä. Kysymykset ovat tutkimuksen liitteenä. Tutkimusta suoritettaessa kysymysrunkoa muutettiin siten, että kaksi ensimmäistä kysymystä jätettiin tutkimuksesta pois, jotta tutkimukseen osallistuneiden anonymiteetti pystyttiin turvaamaan. Pois jäteyty kysymykset kosivat sitä, kauanko henkilöt olivat työskennelleet poliisissa ja rikostutkintayksikössä. Samoin viimeinen kysymys kryptovaluuttojen verotuksesta rajattiin pois, koska tutkimuksen tarkoitus oli tutkia haastateltavien tietämystä koskien kryptovaluuttojen toimintaa, ei niinkään tietämystä niiden verotuksesta. Tutkimuksen tekemiseen täytyi ensin hakea tutkimuslupa Helsingin poliisilaitoksen oikeusyksiköstä, mikä saatiin ennen tutkimuksen tekemistä.

Suoritetussa tutkimuksessa kysymykset 3-13 koskivat haastateltavien omaa näkemystä heidän tietotasostaan koskien kryptovaluuttoja sekä heidän mahdollisia kokemuksia niistä. Samalla kartoitettiin, olivatko haastateltavat saaneet kryptovaluuttoihin liittyvää koulutusta. Kysymykset 14-19 testasivat haastateltavien perustietämystä ilmiöstä. Kysymykset 14-19 pisteytettiin, jotta tutkimustuloksesta sai aikaan näkyvän tuloksen. Pisteytys selviää tutkimuksen liitteenä olevasta tutkimusrungosta.

Kaikilla haastateltavilla oli vähintään muutaman vuoden kokemus työskentelystä Helsingin poliisilaitoksella. Suurin osa haastateltavista oli kokeneita rikostutkijoita, joten tutkimuksen tulosta voidaan pitää varsin pätevänä. Haastateltavien virkanimikkeitä olivat tutkintasihteeri, vanhempi konstaapeli, vanhempi rikoskonstaapeli ja rikosylikonstaapeli. Tutkimukseen osallistui yhteensä 8 haastateltavaa.

6.3 Haastateltavien näkemys omasta tietotasosta koskien kryptovaluuttoja

Kysymys 3. Kuinka syvää katsot tietämyksesi olevan koskien kryptovaluuttoja?

Kuva 8. Pylväsdiagrammi koskien kysymystä 3.

Haastatelluista 4 kertoi, etteivät he tiedä kryptovaluutoista juuri mitään. 4 haastateltavaa kertoi tietävänsä kryptovaluutoista perusasiat. Kukaan haastateltavista ei kokeneet tietävänsä kryptovaluutoista perusasioita enempää.

6.4 Haastateltavien kryptovaluuttojen käyttö

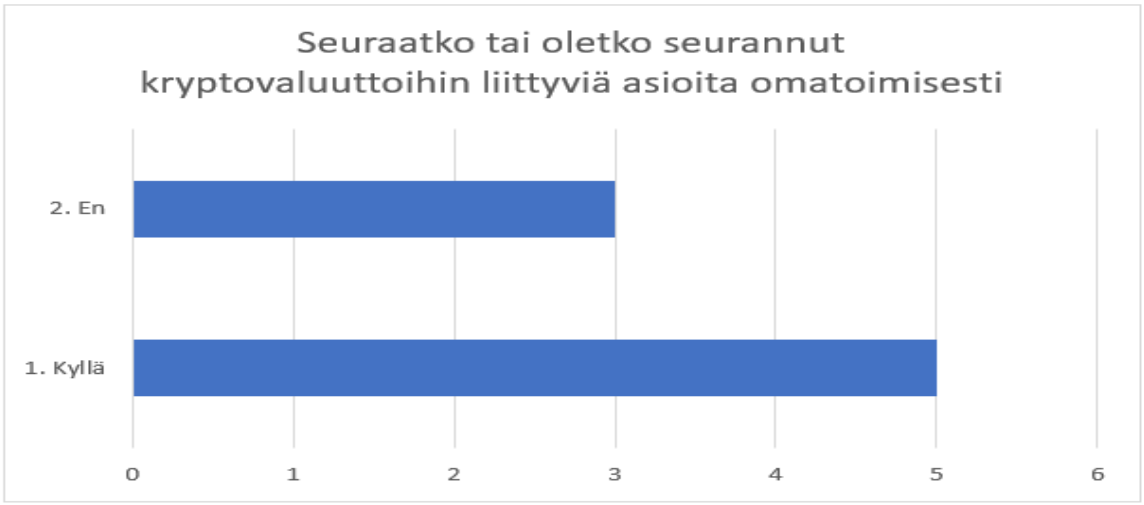
Kysymys 4. oletko joskus sijoittanut kryptovaluuttoihin tai käyttänyt niitä?

Kuva 9. Pylväsdiagrammi koskien kysymystä 4.

Kukaan kahdeksasta haastatellusta ei ollut käyttänyt kryptovaluuttoja tai sijoittanut niihin.

6.5 Haastateltavien perehtyminen kryptovaluuttoihin

Kysymys 5. Seuraatko tai oletko seurannut kryptovaluuttoihin liittyviä asioita omatoimisesti?



Kuva 10. Pylväsdiagrammi koskien kysymystä 5.

Haastatelluista viisi kertoi seuranneensa kryptovaluuttoihin liittyvä asioita omatoimisesti. Kolme haastateltavaa kertoi, etteivät he ole seurannut kryptovaluuttoihin liittyviä asioita omatoimisesti.

6.6 Haastateltavien kryptovaluuttoihin perehtymisen aktiivisuus

Kysymys 6. Mikäli olet, kuinka aktiivisesti?

Kuva 11. Pylväsdiagrammi koskien kysymystä 6.

Kaikki viisi kryptovaluuttoja seurannutta kertoi tutkineensa kryptovaluuttoja vain hieman. Tämä tarkoitti sitä, että he olivat lukeneet kryptovaluuttoihin liittyviä artikkeleja lähinnä sanomalehdistä ja mahdollisesti katsoneet aiheeseen liittyviä videoita. Kukaan ei ollut tutkinut kryptovaluuttoja siten,

että heidän olisi ollut tarkoituksena perehtyä syvällisesti aiheeseen. Kyseessä oli siis suurelta osin melko kevyttä perehtymistä aiheeseen sekä satunnaista aiheeseen liittyvää nettiselailua.

6.7 Haastateltavien törmääminen kryptovaluuttoihin työtehtävissä

Kysymys 7. Oletko törmännyt työtehtäviesi yhteydessä kryptovaluuttoihin?

Kysymys 8. Jos olet, kuinka usein?

Alla yhdistetty kuvaaja kysymyksistä 7-8

Kuva 12. Pylväsdiagrammi koskien kysymyksiä 7-8.

Kaksi haastateltavaa kertoi törmänneensä kryptovaluuttoihin työtehtävissä yli kolme kertaa. Haastatelluista kolme vastasi törmänneensä kryptovaluuttoihin työtehtävien yhteydessä 1-3 kertaa. Yksi haastateltava kertoi törmänneensä kryptovaluuttoihin työtehtävissä yhden kerran ja kaksi haastateltavaa kertoi, etteivät he ole törmänneet kryptovaluuttoihin lainkaan työtehtävien yhteydessä.

Haastateltavat olivat kokonaisuudessaan törmänneet työnkuvassaan kryptovaluuttoihin todella harvoin. Iso osa haastatelluista omasi jo pitkän kokemuksen kyseisen yksikön toiminnasta ja he olivat vuosien saatossa törmänneet kryptovaluuttoihin vain muutamia kertoja. Kyseisessä yksikössä yksittäisen rikostutkijan käsien läpi virtaa vuositasolla parisataa rikosilmoitusta. Ryhmiä johtavien rikosylikonstaapeleiden kautta taas virtaa tuhansia rikosilmoituksia. Näin ollen on nähtävissä, että kyseessä on tutkittavan yksikön kohdalla varsin marginaalinen ilmiö. Osittain tämä saattaa olla seurausta siitä, ettei kyseistä ilmiötä välttämättä tunnisteta, vaikka siihen työtehtävien yhteydessä

törmättäisiinkin. Asia ilmenee myöhemmässä osassa tutkimusta, tietotaitotason kartoituksen yhteydessä.

6.8 Haastateltavien kokemuksia kryptovaluutoista

Kysymys oli suunnattu niille haastateltaville, jotka olivat törmänneet työtehtävien yhteydessä kryptovaluuttoihin. Kysymys kuului seuraavasti.

Menemättä yksityiskohtiin, minkä tyyppisistä tapauksista on ollut kyse. Onko kyseessä ollut petos tyyppisistä tapauksista, kryptovaluuttojen takavarikoinnista vai jotain muuta. Onko kyseessä ollut epäillyn hallussa olleet kryptovaluutat vai asianomistajan?

Tämän kysymyksen ympärille saatiin aikaiseksi mielenkiintoista keskustelua, minkä tulokset käyn tiivistetysti läpi. Kaikkia tapauksia ei käyty läpi vaan ainoastaan keskusteltiin joistakin rikostutkinnoista, joiden yhteydessä haastateltavat olivat törmänneet kryptovaluuttoihin.

Yksi haastatelluista kertoi törmänneensä kryptovaluuttoihin tilanteessa, missä usealta asianomistajalta oli petoksen avulla varastettu perinteistä rahaa. Tapauksesta oli kulunut jo aikaa, eikä haastateltava enää muistanut tarkalleen, miten tapaus eteni. Pääpiirteittäin tapaus oli edennyt kuitenkin seuraavalla tavalla. Asianomistajilta eli rikoksen uhrilta oli varastettu perinteistä rahaa ja noilla rahoilla oli hankittu kryptovaluuttaa epäiltyjen toimisesta. Kryptovaluutat takavarikoitiin rikosprosessin yhteydessä ja oikeus määräsi niistä maksettavan korvaukset asianomistajille. Pienenä yksityiskohtana asiassa haastateltava muisti, että rikosprosessin aikana takavarikoidut kryptovaluutat olivat nostaneet arvoaan ja epäillyt olivat vaatineet oikeudessa asianomistajille maksetun korvauksen ylittävää osaa itselleen. Haastateltava ei muistanut miten asiassa lopulta kävi, mutta oletettavasti korvausten ylittänyt osa maksettiin valtiolle rikoshyötynä.

Toinen haastateltava kertoi rikostutkinnassa tulleen ilmi, että huumekaupan yhteydessä maksut oli suoritettu kryptovaluutalla.

Kolmas haastateltava kertoi yhden tutkinnan liittyneen siihen, että sähköpostin välityksellä oli saatu huijattua asianomistaja siirtämään kryptojaan epäiltyjen haltuun.

Neljäs haastateltava kertoi yhteen tapaukseen liittyneen petokseen, minkä yhteydessä kryptovaluuttaa oli takavarikoitu ja niiden toimintaa oli yritetty rikostutkinnan yhteydessä ymmärtää.

Viides haastateltava kertoi asian liittyneen petokseen.

Kuudes haastateltava kertoi kryptovaluuttoja takavarikoidun joskus.

6.9 Haastateltavien näkemys kryptovaluuttojen esiintymistiheydestä työtehtävissä

Kysymys 10 koski haastateltavien näkemyksiä siitä, ovatko rikostutkinnat mitkä liittyvät jollain tapaa kryptovaluuttoihin lisääntyneet, vähentyneet vai pysyneet ennallaan.

Kuva 13. Pylväsdiagrammi koskien kysymystä 10.

Kaksi vastaajaa kertoi, etteivät he ole törmänneet kryptovaluuttoihin työtehtävien yhteydessä. Kolme vastaaja arvio määrän pysyneen ennallaan. Kaksi vastaajaa katsoi kryptovaluuttojen määrän vähentyneen heidän suorittamien rikostutkintojen yhteydessä ja yksi vastaaja katsoi tapausten lisääntyneen. Vastauksista oli nähtävissä, että kryptovaluuttojen esiintyminen tutkittavan yksikön työnkuvassa oli pysynyt varsin vakiona eli marginaalisena, eikä ilmiö ollut mitenkään erikoisesti nostanut päätään esiin.

6.10 Haastateltavien näkemyksiä kryptovaluuttojen tulevaisuudesta työtehtävissä

Kysymys 11. Näetkö kryptovaluuttojen merkityksen kasvavan nykyisessä työnkuvassasi tulevaisuudessa?

Kuva 14. Pylväsdiagrammi koskien kysymystä 11.

Viisi haastateltavaa koki, että kryptovaluuttojen merkitys tulee kasvamaan heidän työnkuvassaan. Kolme haastateltavaa taas koki, ettei kryptovaluuttojen merkitys tule kasvamaan heidän työnkuvassaan. Mikäli kryptovaluuttojen suosio kasvaa tulevaisuudessa, näkisin niiden merkityksen kasvavan myös kyseisen yksikön työnkuvassa. Muutosta esiintyvyydessä saattaa tapahtua myös erilaisten organisaatiomuutosten kautta ja tutkijakohtaisella tasolla myös esimerkiksi työtehtävien vaihtumisen yhteydessä. Kryptovaluutat myös kehittyvät hurjaa vauhtia, mikä saattaa avata rikolliselle toiminnalle yllättäviäkin vaihtoehtoja. Tällöin voidaan yhtäkkiä olla tilanteessa, missä rikostutkinnassa onkin massoittain kryptovaluuttoihin liittyviä rikostutkintoja käynnissä.

6.11 Haastateltavien näkemyksiä kryptovaluutta tietämyksen tarpeellisuudesta

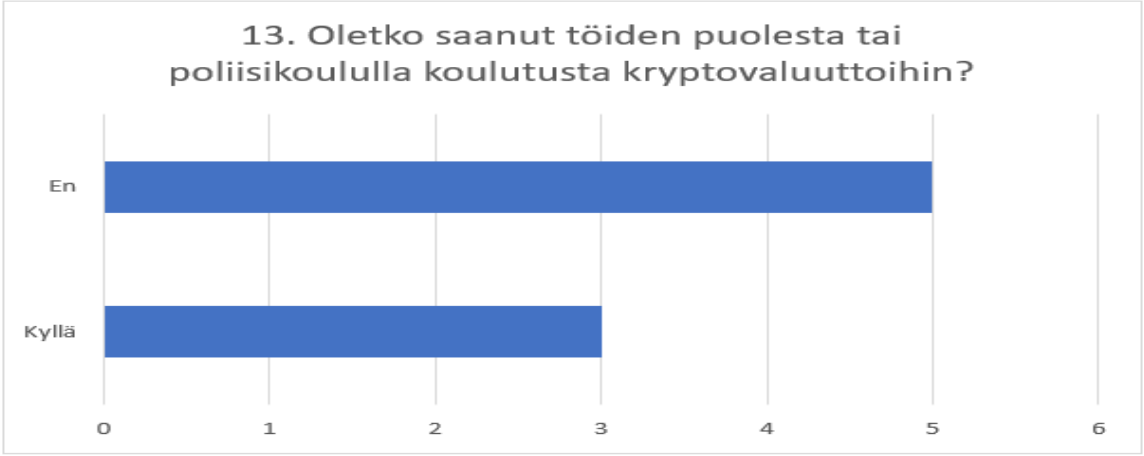
Kysymys 12. Koetko tietämyksen kryptovaluutoista olevan tärkeää nykyisessä työnkuvassasi?

Kuva 15. Pylväsdiagrammi koskien kysymystä 12.

Viisi vastaajaa koki, että tietämys koskien kryptovaluuttoja on tärkeää heidän työnkuvassaan. Kolmen vastaajan mielestä kryptovaluuttatietämyksellä ei ole merkitystä heidän työnkuvassaan. Tällä hetkellä kryptovaluutat muodostavat marginaalisen osuuden kyseisen yksikön työnkuvasta, joten näkökanta on varsin ymmärrettävä ja perusteltu. Tilanne saattaa kuitenkin muuttua, mikäli kryptovaluuttojen käyttö lisääntyy. Tulokseen saattaa vaikuttaa myös se, ettei kryptovaluuttojen toimintaa täysin ymmärretä, eikä niiden tarjoamia mahdollisuuksia esimerkiksi takavarikoiden tekemisen suhteen välttämättä osata nähdä.

6.12 Haastateltavien koulutustausta koskien kryptovaluuttoja

Kysymys 13. Oletko saanut töiden puolesta tai poliisikoululla koulutusta kryptovaluuttoihin?



Kuva 16. Pylväsdiagrammi koskien kysymystä 13.

Kaikkiaan kolme haastateltavaa oli saanut jonkinasteista koulutusta koskien kryptovaluuttoja. Muut eivät olleet saaneet asiaan liittyvä koulutusta.

Tämän kysymyksen jatkokysymys oli suunnattu niille, jotka olivat kertoneet saaneensa koulutusta ja se kuului seuraavasti. Jos olet, onko koulutus ollut itseopiskelua esim. jonkin materiaalin perusteella vai oletko saanut asiaan liittyvä järjestettyä koulutusta?

Kaksi haastateltavaa kertoi saaneensa järjestettyä koulutusta ja yksi kertoi saaneensa koulusta, missä hänelle oli lähetetty sähköposti, jonka sisällä oli ollut aiheeseen liittyvää koulutusmateriaalia. Koulutusta saaneiden tutkimuksen tietotaitotasoa mittaavan kysymysosion kokonaispisteet olivat seuraavat: Vastaajat, jotka olivat saaneet järjestettyä koulutusta: -5/10 ja 2/10 pistettä. Asiaa sähköpostin perusteella opiskelleen vastaajan yhteispisteet olivat -3/10 pistettä. kysymysosion keskiarvopisteet koulutusta saaneiden osalta olivat siis. -2. Muiden haastateltavien pisteet olivat -6, -6, +6, -5, +2. ja heidän kysymysosion keskiarvopisteet olivat 0.6 pistettä. Koulutus on siis ollut tehotonta.

6.13 Mitä haastateltavat tiesivät kryptovaluutoista

Kyselyn tietoperustan hallinta osiossa kysymykset haastateltaville suuntautuivat kryptovaluuttoihin liittyviin perusasioihin. Haastatteluun liittyvä pisteytys ilmenee tutkimuksen liitteenä olevasta kysymysrungosta. Periaatteena oli, että mikäli haastateltava pystyi kertomaan jotain hieman syvällisempää aiheesta, sai hän tietotasonsa mukaan pisteitä väliltä 0-2 ja mikäli haastateltavalla oli heikko

käsitystä kysytystä asiasta sai hän -1 pistettä. Kyselystä pystyi saamaan enimmillään 10 pistettä vastaamalla kaikkiin kysymyksiin riittävällä tarkkuudella. Heikoin mahdollinen kokonaistulos oli puolestaan -6 pistettä. Kyselyn osallistuneista paras pistetulos oli 6 pistettä, heikoimman tuloksen jäädessä -6 pisteeseen. Kaikkien vastanneiden kokonaispisteiden keskiarvo oli -1,875 pistettä. Haastattelun tulos osoittaa, että kahdella haastateltavalla oli jonkinlaista käsitystä tutkittavasta ilmiöstä, mutta muilla haastateltavilla oli melko heikko käsitys kryptovaluutoista tai niiden toimintatavoista. Kysymykset 14-16 ovat listattuna alhaalla. Lisäksi kysymykset löytyvät liitteenä olevasta tutkimusrungosta.

Kysymykset:

14. Pystytkö nimeämään 5 eri kryptovaluuttaa, jos pystyt kerrotko niiden nimet?

15. Tiedätkö, miten kryptovaluuttoja pystyy hankkimaan ja myymään? Mikäli tiedät kerrotko joitain tapoja ja nimeätkö asiaan liittyviä tahoja.

16. Löydät alla olevan listan. Mihin se voisi liittyä, kun puhutaan kryptovaluutoista? (Kyseessä oli kryptovaluuttalompakkoon liittyvä siemenlauselista).

17. Kerrotko, miten kryptovaluuttoja pystyy säilyttämään?

18. Osaatko sanoa miksi yksityinen avain on tärkeä kryptovaluutoissa ja mitä sillä voi tehdä?

19. Mikäli tiedän jonkun henkilön Bitcoin-osoitteen, pystynkö yleisesti ottaen seuraamaan hänen tekemiään siirtoja?

Alla kysymysten 14-19 osalta vastaajakohtaiset kysymyspisteet. Kaavion ylälaidassa näkyy vaakarivillä kunkin kysymyksen 14-19 numerot. Vasemmassa laidassa pystyrivillä näkyy kutakin vastaajaa yksilöivä numero 1-8. Oikealla pystyrivillä näkyy kunkin vastaajan kaikkien kysymysten pisteiden muodostama yhteistulos, missä vastaajakohtaisten kysymysten pistetulokset on laskettu yhteen. Taulukon oikeassa alalaidassa näkyy kaikkien vastanneiden yhteistuloksen keskiarvo, mikä on -1.875 pistettä maksimipisteiden ollessa 10 pistettä.

Kysymys	14	15	16	17	18	19	
	Tulos						Vastaajan kaikkien vastausten yht. ka.
Vastaaja							
1	-1	-1	-1	0	0	0	**-3**
2	1	0	1	0	2	2	**6**
3	-1	-1	-1	0	-1	-1	**-5**
4	-1	0	1	0	2	0	**2**
5	-1	-1	-1	-1	-1	-1	**-6**
6	-1	-1	-1	-1	-1	-1	**-6**
7	1	1	-1	0	2	-1	**2**
8	-1	-1	-1	-1	-1	0	**-5**
Kysymyskohtainen vastausten yht. ka.	**-0.5**	**-0.5**	**-0.5**	**-0.375**	**0.25**	**-0.25**	**-1.875**

Kuva 17. Yhteenvetotaulukko koskien kysymyksiä 14-19.

Paras pistemäärä oli vastaajalla numero 2, hänen saadessa 6/10 pistettä. Heikoimmat pisteet saivat vastaajat 5 ja 6, jotka saivat molemmat -6/10 pistettä eli heikoimman mahdollisen tuloksen.

Alla olevaan taulukkoon on merkitty vihreällä ja keltaisella esiin vastaajat, jotka olivat saaneet koulutusta kryptovaluutoista. Vihreällä merkityt kaksi vastaajat ovat saaneet järjestettyä koulutusta. Keltaisella merkitty yksi vastaaja on itseopiskellut aihetta sähköpostiin lähetetyn koulutusmateriaalin avulla. Muut viisi vastaajat eivät olleet saaneet lainkaan asiaan liittyvää koulutusta.

Kysymys	14	15	16	17	18	19	
Tulos							Vastaajan kaikkien vastausten yht. ka.
Vastaaja							
1	-1	-1	-1	0	0	0	**-3**
2	1	0	1	0	2	2	**6**
3	-1	-1	-1	0	-1	-1	**-5**
4	-1	0	1	0	2	0	**2**
5	-1	-1	-1	-1	-1	-1	**-6**
6	-1	-1	-1	-1	-1	-1	**-6**
7	1	1	-1	0	2	-1	**2**
8	-1	-1	-1	-1	-1	0	**-5**
Kysymyskohtainen vastausten yht. ka.	**-0.5**	**-0.5**	**-0.5**	**-0.375**	**0.25**	**-0.25**	**-1.875**

Kuva 18. Yhteenvetotaulukko koskien vastaajien saamaa koulutusta.

Tuloksesta on nähtävissä, ettei kumpikaan koulutustapa ole ollut kovinkaan tehokas. Järjestettyä koulutusta saaneiden yhteispisteet olivat -5 ja 2. Itseopiskelumateriaalin perusteella koulutusta saaneen henkilön pisteiden yhteistulos oli -3 pistettä.

Alla olevassa taulukossa on punaisella merkitty ne kolme vastaajaa, jotka ovat haastattelussa kertoneet törmänneensä työtehtävien yhteydessä kryptovaluuttoihin yli 3 kertaa. Ruskealla on merkattu ne kaksi vastaaja, jotka olivat törmänneet kryptovaluuttoihin 1-3 kertaa. Vaalean ruskealla on merkattu vastaaja, joka kertoi törmänneensä kryptovaluuttoihin yhden kerran. Valkoisella on merkitty ne kaksi vastaaja, jotka eivät olleet törmänneet kryptovaluuttoihin työtehtävien yhteydessä.

Kysymys	14	15	16	17	18	19	
	Tulos						Vastaajan kaikkien vastausten yht. ka.
Vastaaja							
1	-1	-1	-1	0	0	0	-3
2	1	0	1	0	2	2	6
3	-1	-1	-1	0	-1	-1	-5
4	-1	0	1	0	2	0	2
5	-1	-1	-1	-1	-1	-1	-6
6	-1	-1	-1	-1	-1	-1	-6
7	1	1	-1	0	2	-1	2
8	-1	-1	-1	-1	-1	0	-5
Kysymyskohtainen vastausten yht. ka.	-0.5	-0.5	-0.5	-0.375	0.25	-0.25	-1.875

Kuva 19. Yhteenvetotaulukko koskien vastaajien törmäämistä kryptovaluuttoihin.

Tuloksen mukaan ne vastaajat, jotka kertoivat törmänneensä kryptovaluuttoihin eniten, saivat kyselyn heikoimpia pisteitä. Tulos on kokonaisuudessaan yllättävä.

Vastaaja numero 3 oli törmännyt työssään kryptovaluuttoihin yli kolme kertaa, ja hän oli myös saanut aiheeseen liittyvää järjestettyä koulutusta mutta tästä huolimatta hänen kyselystä saamansa pisteet olivat heikot. Edellä mainittu kertoo siitä, kuinka vaikeasti ymmärrettävästä asiasta on kyse.

Haastattelun yhteydessä ei tarkemmin käyty läpi, miten kryptovaluuttoihin liittyneet rikostutkinnat oli tutkinnallisesti hoidettu. Tutkimuksen tuloksen perusteella pidän kuitenkin todennäköisenä, että näissä tapauksissa on pyydetty tutkinta-apua jostain toisista rikostutkintayksiköistä, missä tietotaitoa ilmiön suhteen on löytynyt enemmän. Toinen vaihtoehto voi olla, että kryptovaluuttoihin liittyviä rikostutkintoja on hoidettu ryhmänä, jolloin joku ryhmän jäsen on perehtynyt asiaan syvemmin muiden hoitaessa muita kyseiseen rikostutkintaan liittyviä asioita. Asiaan voi vaikuttaa myös se, että esimerkiksi rikosylikonstaapelit eivät välttämättä hoida rikoksiin liittyviä tutkintoja kovinkaan konkreettisesti, vaan he jakavat tutkittavat jutut rikostutkijoille ja johtavat sekä ohjaavat tutkintaa rikostutkijoiden heille esittämien selontekojen ja kysymysten jälkeen. Kryptovaluuttoihin liittyneet tutkinnat on saatettu myös siirtää kokonaan tai osittain toisiin rikostutkintayksiköihin alkukartoituksen jälkeen. Osaltaan asiaan saattaa vaikuttaa myös se, että kyseisitä rikoksista ja koulutuksesta on voinut kulua jo pidempi aika, jolloin asiat ovat saattaneet unohtua.

7 Pohdinta

Lainsäädäntö antaa varsin hyvät ja kattavat valtuudet poliisille suorittaa erilaisia etsintöjä tutkittaviin rikoksiin liittyen sekä takavarikoiden ja vakuustakavarikon suorittamiseen suhteen. Laki sallii myös laite-etsinnän suorittamisen jo melko lievissä rikoksissa. Mielestäni kryptovaluuttoihin liittyvien perusasioiden hallinta olisi syytä olla kohtalaisella tasolla myös ns. peruspoliisitoiminnassa. Kryptovaluutat ovat ainakin suurimpien kryptovaluuttojen osalta likvidiä omaisuutta ja ne voivat olla suhteellisen helposti takavarikoitavissa, mikäli asiaan liittyvät toimintamekanismit, ohjelmat sekä toimijat ovat tutkivan viranomaisen tuntemia. Kryptovaluuttoihin liittyy vahvasti se, että niiden haltijan täytyy itse huolehtia salasanoista ja muista asiaan liittyvistä seikoista, jolloin salasanoista ym. otetaan usein kuvia tai niitä säilytetään esimerkiksi paperilla tai niistä tehdään muita merkintöjä. Näin ollen laite-etsintöjen, henkilötarkastusten sekä koti- ja paikkaetsintöjen avulla on suuri mahdollisuus saada takavarikoitua henkilön hallussa olevaa kryptovaluutta omaisuutta.

Vakuustakavarikoiden osalta voidaan todeta, että mikäli rikostutkinnan yhteydessä päädytään takavarikoimaan henkilön hallusta kryptovaluuttoja, täytyy rikoksen näyttö olla vahvaa, jotta asia menestyy oikeudessa. Muutoin on olemassa suuri riski sille, että valtio määrätään maksamaan korvauksia henkilölle, kenen hallusta kryptovaluutat on vakuustakavarikoitu. Samoin on syytä arvioida sitä, kuinka paljon kryptovaluuttoja takavarikoidaan ja ottaa huomioon niiden mahdollinen voimakaskin arvon vaihtelu. Takavarikonnin yhteydessä myös kryptovaluuttoihin liittyvät siirtomaksut täytyy huomioida, koska ne saattavat muodostua suhteellisen suuriksi etenkin siirrettäessä Ethereum-alustan päällä NFT-tokeneita tai siirrettäessä arvoltaan pieniä määriä kryptovaluuttaa.

Takavarikoitujen kryptovaluuttojen säilytysratkaisut tulisi kartoittaa tarkasti, koska on olemassa eroavaisuuksia siinä, mitä kryptovaluuttaa kussakin kryptovaluuttalompakossa pystyy säilyttämään. Itse siirroissa on noudatettava suurta huolellisuutta, koska siirtoihin voi liittyä suuria eroavaisuuksia eri kryptovaluuttojen välillä. Myös lompakkojen hallintaan tulee kiinnittää huomiota.

Rikostorjuntayksikön henkilöstön keskuudessa oli havaittavissa puutteita kryptovaluuttoihin liittyvien perusasioiden hallinnassa. Osa haastatelluista oli saanut jonkin asteista koulutusta ilmiöön liittyen, mutta koulutus on ollut selkeästi riittämätöntä. Mikäli kyseinen ilmiö halutaan tunnistaa rikostutkinnan yhteydessä, voisi harkittavaksi tulla, että sen ympärille luotaisiin järjestettyä koulutusta. Kryptovaluutat ovat laaja ja monimutkainen ilmiö. Mikäli yksikön työntekijöiden tietotaidon tasoa koskien kryptovaluuttoja halutaan nostaa, lienee järjestetty koulutus paras vaihtoehto. Ilmiön itseopiskelu pelkän opetusmateriaalin perusteella voi olla haastavaa ilman työntekijän omaa sisäsyntyistä kiinnostusta aiheeseen.

Mielestäni aiheesta olisi hyvä tehdä jatkotutkimus, missä selvitettäisiin, kuinka kryptovaluuttoihin liittyviä asioita voitaisiin kouluttaa tutkitussa yksikössä helpoiten ja tehokkaasti siten, että koulutus tukisi yksikön toimintaa. Toinen jatkotutkimuksen aihe voisi olla, kuinka luoda kryptovaluuttoihin liittyvää helposti omaksuttavaa opetusmateriaalia.

Tutkimustulos kertoo sen, että kyseinen ilmiö tiedetään tutkittavassa yksikössä mutta sitä ei välttämättä osata tunnistaa ja ilmiön perusasioiden hallinnassa on puutteita. Tutkimustulos kertoo ilmiön muodostavan varsin marginaalisen osan tutkittavan yksikön työnkuvasta. Osin tämä saattaa johtua siitä, ettei ilmiötä tunnisteta tai hallita. Ilmiön selkeästi marginaalisen esiintyvyyden vuoksi on tärkeää harkita, kuinka paljon sen mahdolliseen kouluttamiseen satsataan. Tykillä ei kannata ampua kärpästä, muistaen kuitenkin kryptovaluuttojen olevan nopeasti kehittyvää teknologiaa, mikä voi tuoda yllätyksiä eteen esimerkiksi pinnalle pulpahtavina rikosilmiöinä.

Tutkitun yksikön henkilöstön olisi hyvä tiedostaa kryptovaluuttoihin liittyvät menettelytavat eli mihin toimenpiteisiin ryhdytään, mikäli ilmiö tunnistetaan työtehtävien yhteydessä. Kryptovaluuttojen monimutkaisuuden sekä vähäisen esiintyvyyden vuoksi ei voida olettaa kaikkien yksikön työntekijöiden ymmärtävän niitä syvällisesti, mutta olisi hyvä, mikäli ilmiön tunnistamisen jälkeen voitaisiin jatkaa jonkin vakiintuneen prosessin kautta aisan eteenpäin viemistä.

Tutkimuksen tekijällä ei ole tiedossa, onko kyseisessä yksikössä jo käytössä edellä mainittuja toimenpiteitä tai prosesseja. Kyseistä asiaa olisi ollut hyvä selvittää tutkimuksen tekemisen yhteydessä, mutta asia tuli tutkimuksen tekijän mieleen havaintona, vasta tutkimustuloksen läpikäymisen yhteydessä. Yksi vaihtoehto voisi olla aiheeseen hieman syvällisemmin perehtyneiden yhteyshenkilöiden kouluttaminen joiden apuun työntekijät voisivat tarvittaessa turvautua, mikäli ilmiö havaitaan työtehtävien yhteydessä.

Koin onnistuneeni tutkimuksen tekemisen yhteydessä. Aihe oli haastavampi, kuin mitä ennalta ajattelin. Suurimpana ongelmana tutkimuksen tekemisen yhteydessä olivat aiheen laajuus sekä osittaiset puutteet ennakkovalmistelussa. Tutkimusta olisi pitänyt miettiä syvällisemmin ja järjestelmällisemmin heti alusta saakka. Tutkimuksen tekeminen toimi kuitenkin hyvänä oppimisprosessina ja koin oppineeni paljon tutkimuksen tekemisen yhteydessä. Tutkimuksen kautta sain mielestäni tuotua selkeästi esiin tutkimustulokset. Tutkimus on laadittu sellaisessa muodossa, että sen pystyy tarvittaessa toistamaan.

Tutkimuksesta rajattiin pois myös useita mielenkiintoisia kryptovaluuttoihin liittyviä aiheita niiden laajuuden vuoksi, kuten kryptovaluuttojen jäljittäminen ja niihin liittyvät tietopyynnöt. Rajatuista aiheista olisi varsin mielenkiinoista tehdä omat tutkimuksensa. Myös kryptovaluuttojen mahdollisia tulevaisuuden kehityssuuntia olisi hyvä tutkia rikostukinnan näkökannalta katsottuna.

Lähteet

Andersen, D. 2023. US Justice Department investigating Binance for violating Russian sanctions: Report. Luettavissa: https://cointelegraph.com/news/us-justice-department-investigating-binance-for-violating-russian-sanctions-report. Luettu:06.05.2023.

Ammous, S. 2018. The Bitcoin Standard. John Wiley & Sons, Inc. E-kirja. Luettu:20.1.2023

Bashir, I. 2022. Blockchain Consensus. Apress. Lontoo. E-kirja. Luettu:30.2.2023

Bertaccini, M. 2022. Cryptography Algorithms. Packt Publishing ltd. Birmingham. E-kirja. Birmingham. Luettu:30.03.2023.

Binance 2023a. Token. Luettavissa: https://academy.binance.com/en/glossary/token.Luettu: 04.04.2023.

Binance 2023b. Airdrop. Luettavissa: https://academy.binance.com/en/glossary/airdrop. Luettu: 04.04.2023.

Bitpay 2023. 4 Easy Ways to Convert Bitcoin to Cash. Luettavissa: https://bitpay.com/blog/cash-out-bitcoin/. Luettu:4.3.2023.

Blockchain.com 2023. Luettavissa: https://www.blockchain.com/explorer/transactions/btc/ec8a9fdff473e9b2f368b8cb1f7c9b2b7099b6b8fafa263134e887d2cdb95fb2. Luettu 03.03.2023.

Blocknative 2022. A Staker's Guide to Ethereum Slashing & Other Penalties. Luettavissa: https://www.blocknative.com/blog/an-ethereum-stakers-guide-to-slashing-other-penalties. Luettu: 04.04.2023.

Bosworth A, Clegg N. 2021. Building the Metaverse Responsibly. Luettavissa: https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/. Luettu:08.05.2023.

Brave 2023. Brave Rewards. Luettavissa: https://brave.com/brave-rewards/. Luettu: 04.04.2023.

Btc.com. Luettavissa: https://explorer.btc.com/btc/block/779148. Luettu: 03.03.2023.

Caetano, R. 2015. Learning Bitcoin. Packt Publishing. E-kirja. Luettu:02.05.2023.

Chainanalysis 2023. The 2023 Crypto Crime Report. Luettavissa: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf. Luettu:30.04.2023.

Chainlink 2023. What Are Automated Market Makers (AMMs)?. Luettavissa: https://chain.link/education-hub/what-is-an-automated-market-maker-amm. Luettu: 04.04.2023.

Cointelegraph 2023. Proof-of-stake vs. proof-of-work: Pros, cons, and differences explained. Luettavissa: https://cointelegraph.com/learn/proof-of-stake-vs-proof-of-work:-differences-explained. Luettu: 04.04.2023.

Cointelegraph s.a. A beginner's guide to buying virtual real estate in Decentraland (MANA). Luettavissa:https://cointelegraph.com/learn/a-beginners-guide-to-buying-virtual-real-estate-in-decentraland-mana. Luettu:08.05.2023.

Coinmarketcap s.a. Today's Cryptocurrency Prices by Market Cap. Luettavisa: https://coinmarketcap.com/ Luettu:22.10.2022.

Trozze, A. Kamps, J. Akartuna, E. Hetzel, F. Kleinberg, B .2022. Cryptocurrencies and future fnancial crime. Crime Science, Heidelberg Vol. 11. Issue. 1. Luettu: 08.05.2023.

Ethereum 2022. INTRODUCTION TO SMART CONTRACTS. Luettavissa: https://ethereum.org/en/developers/docs/smart-contracts/. Luettu: 04.04.2023.

Ethereum 2023a. INTRO TO ETHEREUM. Luettavissa: https://ethereum.org/en/developers/docs/intro-to-ethereum/. Luettu:04.04.2023.

Ethereum 2023b. ERC-20 TOKEN STANDARD. Luettavissa: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/. Luettu: 12..03.2023.

Ethereum 2023c. ERC-721 NON-FUNGIBLE TOKEN STANDARD. Luettavissa: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/. Luettu: 12.03.2023.

Ethereum 2023d. ETHEREUM VIRTUAL MACHINE (EVM). Luettavissa: https://ethereum.org/en/developers/docs/evm/. Luettu: 04.04.2023.

Euripol 2021. Crryptocurrencies. Traking. Luettavissa: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf. Luettu: 11.03.2023.

Frankenfield J, 2021. Luettavissa: Public Key. https://www.investopedia.com/terms/p/publickey.asp. Luettu: 29.03.2023.

Frankenfield, J. 2022a. What Is Altcoin? Luettavissa: https://www.investopedia.com/terms/a/altcoin.asp. Luettu:03.05.2023.

Frankfield, J. 2022b. 51% Attack: Definition, Who Is At Risk, Example, and Cost. Luettavissa: https://www.investopedia.com/terms/1/51-attack.asp Luettu:23.10.2022.

Frankenfield, J. 2023a. What Are Smart Contracts on the Blockchain and How They Work. Luettavissa: https://www.investopedia.com/terms/s/smart-contracts.asp. Luettu:22.03.2023.

Frankenfield, J. 2023b.Bitcoin Mining. Luettavissa: https://www.investopedia.com/terms/b/bitcoin-mining.asp. Luettu:07.05.2023.

George, K. 2023. Cryptocurrency Regulations Around the World. Luettavissa: https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122. Luettu:08.05.2023.

Hendrickson, R & Luther, W. 2022. Cash, crime, and cryptocurrencies. The Quarterly Review of Economics and Finance. Volume 85, Pages 200-207.

Hyppönen, A. 2022a. Mikä on kryptovaluutta. Luettavissa: https://bitcoinkeskus.com/kryptovaluutta/: Luettu 12.03.2023.

Hyppönen, A. 2023b. Kryptovaluuttalompakko – aloittelijan opas. Luettavissa: https://bitcoinkeskus.com/kryptovaluutta-lompakko/. Luettu: 03.04.2023.

Jeans D, Emerson S. 2022. The Devil In Nerd's Clothes': How Sam Bankman-Fried's Cult Of Genius Fooled Everyone. Luettavissa: https://www.forbes.com/sites/davidjeans/2022/11/12/the-devil-in-nerds-clothes-how-sam-bankman-frieds-cult-of-genius-fooled-everyone/?sh=56a9187e1d26. Luettu:04.04.2023.

Korkein oikeus. 2023. KKO:2022:75. Luettavissa: https://korkeinoikeus.fi/fi/index/ennakkopaatokset/kko202275.html. Luettu:20.03.2023.

Kyberturvallisuuskeskus. 2020. SHA-1-tiivistefunktio on lopullisesti murrettu. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sha-1-tiivistefunktio-lopullisesti-murrettu. Luettu:07.05.2023.

Li, Y & Wang, C. 2022. A search-theoretic model of double-spending fraud. Journal of Economic Dynamics and Control. Volume 142.

Linnake, T. 2021.Poliisia työllistävät uudenlaiset huijaukset, rahoja ei saa takaisin – "Ihmisille syntyy jonkinlainen sokeus". Luettavissa: https://www.is.fi/digitoday/art-2000008409074.html. Luettu:08.05.2023.

Lyons, H. 2022. NFTs seized by police for the first time ever in Belgium. Luettavissa: https://www.brusselstimes.com/234830/nfts-seized-by-police-for-the-first-time-ever-in-belgium. Luettu: 04.04.2023.

Mocc 2022. Tietokoneen toiminnan perusteet 2022. Luettavissa: https://tito-perusteet-2022.mooc.fi/luku-3/1-tiedon-kategoriat. Luettu: 03.03.2023.

moreReese 2022. How the Bitcoin Network is Maintained. Luettavissa: https://decrypt.co/resources/what-are-the-different-types-of-bitcoin-nodes-how-the-bitcoin-network-is-maintained Luettu: 19.10.2022.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Luettavissa: https://bitcoin.org/bitcoin.pdf. Luettu: 29.04.2023.

Napoletano, E. 2023. Forbes Advisor. Proof Of Stake Explained. Luettavissa: https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake/. Luettu:29.03.2023.

Oikeudenkäymiskaari 1.1.1734/4.

Pakkokeinolaki 22.7.2011/806.

Passwordgenerator.net. Luettavissa: https://passwordsgenerator.net/sha256-hash-generator/. Luettu: 03.03.2023.

Poliisi 2020. Helsingin poliisi on tutkinut satoja suljetulla Silkkitiellä tehtyjä huumekauppoja – huumausainerikoksista epäillään yli kolmeasataa ostajaa. Luettavissa: https://poliisi.fi/-/helsingin-poliisi-on-tutkinut-satoja-suljetulla-silkkitiella-tehtyja-huumekauppoja-huumausainerikoksista-epaillaan-yli-kolmeasataa-ostajaa. Luettu:06.05.2023.

Poliisi s.a. Helsingin poliisilaitoksen organisaatio. Luettavissa: https://poliisi.fi/organisaatio-ja-johto-helsingin-poliisilaitos. Luettu: 09.05.2023.

Quinones, A., Nakamoto, S. 2021. Bitcoin ja Monero Kryptovaluuttojen kuninkaat. Oppian. Helsinki.

Reiff, N. 2021. What Are Centralized Cryptocurrency Exchanges? Luettavissa: https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/. Luettu:04.04.2023.

Reiff, N 2022. What Was the First Cryptocurrency? Luettavissa: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/. Luettu:29.03.2023.

Saad, M. Qin, Z. Ren, K. Nyang, D. Mohaisene, D. 2021. PoS: Making Proof-of-Stake Decentralized and Fair. EEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 32, NO. 8.

Saqan, S. 2022. Explanation of Bitcoin's Elliptic Curve Digital Signature Algorithm. Luettavissa: https://suhailsaqan.medium.com/explanation-of-bitcoins-elliptic-curve-digital-signature-algorithm-6603f951863a. Luettu 30.04.2023.

Salumäki, T. 2015. Poliisi napannut rikollisilta jo jättisumman bitcoineja. Luettavissa: https://yle.fi/a/3-8410869. Luettu:07.05.2023.

Scheneier, B. 2015. Applied cryptography, protocols, algoritmes and source code in C. 20th anniversary edition. E-kirja. Luettu:18.10.2022.

Szmigielski, A. 2016. Bitcoin Essentials, Packt Publishing. E-kirja. Luettu:18.12.2022.

The Blockchain Guy 2022. Protect Your Blockchain Identity | Tornado Cash Tutorial. Katsottavissa: https://www.youtube.com/watch?v=vytsfgbyi88. Katsottu:01.05.2023.

Tilastokeskus 2022. Tietoon tulleet rikokset ja niiden selvittäminen rikosryhmittäin tekokunnan ja ilmoitusvuoden mukaan, 1980-2021. Luettavissa: https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__rpk/statfin_rpk_pxt_13ex.px/. Luettu:09.05.2023.

United States Attorney's Office Eastern District of Michigan 2023. FBI DISRUPTS VIRTUAL CURRENCY EXCHANGES USED TO FACILITATE CRIMINAL ACTIVITY. Luettavissa: https://www.justice.gov/usao-edmi/pr/fbi-disrupts-virtual-currency-exchanges-used-facilitate-criminal-activity. Luettu:06.05.2023.

U.S. DEPARTMENT OF THE TREASURY 2022. U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Luettavissa: https://home.treasury.gov/news/press-releases/jy0916. Luettu:30.04.2023.

Valtionvarainministeriö s.a. Valtion budjetti. Luettavissa: https://vm.fi/valtion-budjetti. Luettu: 10.05.2023.

Välimaa, M. 2018. Bitcoineja poliisille 700 000 euron arvosta – Rattijuopon pidätys Espoossa johti laajaan huumetutkintaan: Satoja ostajia ympäri Suomea. Luettavissa: https://www.lansivayla.fi/paikalliset/1475352. Luettu:07.05.2023.

Wikipedia s.a. Helsinki. Luettavissa: https://fi.wikipedia.org/wiki/Helsinki. Luettu:09.05.2023.

ZenGo. 2020. Unveiling BigSpender: Double (and Multiple) Spend Vulnerability in Major Bitcoin Wallets. Luettavissa: https://zengo.com/bigspender-double-spend-vulnerability-in-bitcoin-wallets/.Luettu:06.05.2023.

Liitteet

Liite 1. Kysymysrunko

Esitettävät tutkimuskysymykset haastattelun yhteydessä

Taustatietoa

Tutkimuskysymykset:

1. **Kuinka kauan olet työskennellyt poliisissa?**

Alle 5 v

5-10 v.

Yli 10 v.

2. **Kuinka kauan olet työskennellyt rikostorjuntayksikössä?**

Alle vuoden

1-5 vuotta

5-10 vuotta

Yli 10 vuotta

3. **Kuinka syvää katsot tietämyksesi olevan koskien kryptovaluuttoja?**

Olen mahdollisesti kuullut puhuttavan niistä, mutta en tiedä niistä oikeastaan mitään.

Tiedän perusasiat

Tiedän paljon

Tietämykseni on ammattitasoa

4. **Oletko joskus sijoittanut kryptovaluuttoihin tai käyttänyt niitä?**

Kyllä/En

5. **Seuraatko tai oletko seurannut kryptovaluuttoihin liittyviä asioita omatoimisesti?**

Kyllä/En

6. **Mikäli olet, kuinka aktiivisesti?**

Olen perehtynyt niihin hieman omatoimisesti eli olen esim. lueskellut niistä tai katsonut jonkun videon.

Olen tutkinut kryptovaluuttoja aktiivisesti.

7. **Oletko törmännyt työtehtäviesi yhteydessä kryptovaluuttoihin?**

Kyllä/En

8. **Jos olet kuinka usein**

Yhden kerran

1-3 kertaa

Yli kolme kertaa

9. **Kysymys henkilöille, jotka ovat törmänneet työtehtävissä kryptovaluuttoihin. Menemättä yksityiskohtiin, minkä tyyppisistä tapauksista on ollut kyse. Onko kyseessä ollut petos tyyppisistä tapauksista, kryptovaluuttojen takavarikoinnista vai jotain muuta. Onko kyseessä ollut rikoksesta epäillyn hallussa olleet kryptovaluutat vai asianomistajan?**

10. **Mikä on näkemyksesi?**

Kryptovaluutat ovat tulleet kasvavassa määrin esiin työnkuvassani.

Kryptovaluutat ovat tulleet vähenevässä määrin esiin työnkuvassani.

Kryptovaluuttoihin törmääminen on pysynyt ennallaan työnkuvassani.

En ole törmännyt kryptovaluuttoihin työnkuvassani

11. Näetkö kryptovaluuttojen merkityksen kasvavan nykyisessä työnkuvassasi tulevaisuudessa?

Kyllä/en

12. Koetko tietämyksen kryptovaluutoista olevan tärkeää nykyisessä työnkuvassasi?

Kyllä/En

13. Oletko saanut töiden puolesta tai poliisikoululla koulutusta kryptovaluuttoihin?

Kyllä/en

Jos olet, onko koulutus ollut itseopiskelua esim. jonkin materiaalin perusteella vai oletko saanut asiaan liittyvää järjestettyä koulutusta?

Itseopiskelua/järjestettyä koulutusta

Perusasioiden hallinta

14. Pystytkö nimeämään 5 eri kryptovaluuttaa, jos pystyt kerrotko niiden nimet?

-1 piste ellei pysty +1 jos pystyy.

15. Tiedätkö, miten kryptovaluuttoja pystyy hankkimaan ja myymään. Mikäli tiedät kerrotko joitain tapoja ja nimeätkö asiaan liittyviä tahoja?

-1p. mikäli ei pysty sanomaan mitään, 0p mikäli kertoo, että pörssistä, mutta ei osaa nimetä mitään pörssiä, +1 mikäli pystyy nimeään jonkin keskitetyn pörssin +2p mikäli pystyy kertomaan jonkin eri tavan pörssin lisäksi: louhinta, airdrop, faucet, steikkaus, ansaitseminen esim. brave selain tai osaa kertoa jonkin hajautetun pörssin, mistä voi hankkia. Eli +2p mikäli osoittaa hieman syvempää tietämystä.

16. Löydät alla olevan listan. Mihin se voisi liittyä, kun puhutaan kryptovaluutoista?

cloud dad ink computer paper lamb sheep dog window car

girl flower mat ice sofa helmet stairs star fireplace roof

Lompakon siemenlauseet

-1 mikäli ei osaa keroa +1 mikäli osaa kertoa.

17. Kerrotko miten kryptovaluuttoja pystyy säilyttämään?

-1 mikäli ei osaa sanoa mitään.0 mikäli osaa sanoa pörssissä tai lompakossa +1 mikäli osaa nimetä joitain lompakoita, esim. metamask tms. +2 mikäli osaa kertoa esim. paperille, laitelompakot…

18. Osaatko sanoa, miksi yksityinen avain on tärkeä kryptovaluutoissa ja mitä sillä voi tehdä?

-1 mikäli ei osaa kertoa. + 2 mikäli osaa kertoa

19. Mikäli tiedän jonkun henkilön bitcoin osoitteen, pystynkö yleisesti ottaen seuraamaan hänen tekemiään siirtoja?

-1 Jos vastaa väärin. 0 jos vastaa oikein. +2 mikäli osaa kertoa miten asia tapahtuu suurin piirtein.

20. Käyt kauppaa kryptovaluutoilla. Milloin sinun täytyy maksaa veroja?

-1 mikäli ei osaa kertoa. 0 jos jotain hajua +2 mikäli oikein.