

Kryptovaluuttojen louhinnan ekosysteemi

Andrei Saltõkov



Tekijä(t) Andrei Saltökov	
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Raportin/Opinnäytetyön nimi Kryptovaluuttojen louhinnan ekosysteemi	Sivu- ja liitesivumäärä 34 + 6
<p>Tässä opinnäytetyössä tarkastellaan kaivostoimintaa ilmiönä ja käsitellään siihen liittyvää ekosysteemiä.</p> <p>Teoreettisessa osassa käsitellään louhintatoiminnan (eli kaivostoiminnan) ekosysteemin elementtejä, kuten: lohkoketju ja kryptovaluutta, kaivostoiminnan laitteisto ja ohjelmisto, infrastruktuuri.</p> <p>Opinnäytetyön empiirisessä osassa esitetään kyselyn tutkimustulokset. Kysely järjestettiin kaivostoimintaan liittyvien ihmisten kesken, jotka ovat myös suurimpien yhtiöiden jäseniä sellaisilla Internet-paikoilla, kuten Internet-foorumit, sosiaalisten verkostojen ryhmät ja YouTube:n kanavat. Tämän kyselyn päätavoitteena on löytää tehokkaita välineitä kryptovaluuttojen kaivostoimintaa varten ottaen huomioon yhteisön mielipiteen.</p> <p>Viimeisessä osassa tai loppupohdinnassa tehdään päätelmät tutkimuksen pohjalta optimaalisesta kaivoslaitteistosta ja laitteiden ominaisuuksista.</p> <p>Tämän opinnäytetyön tavoitteena ei ole positiivisen tai negatiivisen mielipiteen muodostaminen kryptovaluuttojen louhinnasta. Tässä opinnäytetyössä ei arvioida kryptovaluuttojen louhintaan liittyviä riskejä. Suoritetusta tutkimuksesta saadut tulokset ja tehdyt johtopäätökset saattavat olla vain suositusluonteisia, koska tämän opinnäytetyön tarkoitus ei ole laboratoriotutkimuksen tulosten vahvistaminen.</p>	
Asiasanat Kryptovaluutta, kyselytutkimus, kryptovaluutan louhinta, lohkoketju, ekosysteemi	

Sisällys

1	Johdanto	1
2	Perusteknologia	3
2.1	Kryptovaluutta	3
2.2	Lohkoketju	4
3	Kryptovaluutan louhintalaitteisto	7
3.1	ASIC louhintalaite	7
3.2	GPU louhintalaite	8
4	Ohjelmisto louhintatoimintaa varten.....	9
4.1	Klassiset käyttöjärjestelmät.....	9
4.1.1	Microsoft Windows	10
4.1.2	Linux-pohjaiset käyttöjärjestelmät	10
4.2	Käyttöjärjestelmät louhintatoiminta varten	11
4.2.1	Käyttöjärjestelmä ethOS.....	11
4.2.2	Käyttöjärjestelmä PiMP OS (Portable Instant Mining Platform).....	11
4.2.3	Käyttöjärjestelmä SimpleMining OS	12
4.3	Louhinnan asiakasohjelmat.....	12
4.4	Ohjelmisto optimointiin ja mukauttamiseen	13
5	Infrastruktuuri	14
5.1	Kaivosallas.....	14
5.2	Kryptovaluuttojen pörssi.....	15
5.3	Kryptolompakko	16
6	Tutkimus	18
6.1	Tutkimusmenetelmät.....	18
6.2	Kyselylomakkeen rakenne	19
6.3	Tutkimustulokset	20
6.3.1	Vastaajien sukupuoli	20
6.3.2	Vastaajien ikä.....	20
6.3.3	Vastaajien kokemukset kryptovaluuttojen louhintatoiminnasta	20
6.3.4	Vastaajien taitojen arviointi kryptovaluuttojen louhintatoiminnan alalla	21
6.3.5	Henkilökohtainen suhtautuminen louhintatoimintaan.....	21
6.3.6	Kryptovaluuttojen louhintatoiminnan tulevaisuuden arviointi.....	22
6.3.7	Laitteet	22
6.3.8	Laitteiden ominaisuudet	23
6.3.9	Käyttöjärjestelmät.....	24
6.3.10	Käyttöjärjestelmien ominaisuudet.....	24
6.3.11	Client-ohjelmisto	25
6.3.12	Client-ohjelmiston ominaisuudet.....	25

6.3.13 Optimointiohjelmistot.....	26
6.3.14 Kaivosaltaat	27
6.3.15 Kaivosaltaiden ominaisuudet.....	27
6.3.16 Kryptovaluuttojen pörssi	28
6.3.17 Kryptovaluuttojen pörskien ominaisuudet	29
6.3.18 Kryptolompakot	29
6.3.19 Kryptolompakoiden ominaisuudet	30
7 Pohdinta.....	31
7.1 Tulosten luotettavuus	31
7.2 Johtopäätökset.....	31
7.3 Jatkokehitys- ja tutkimusehdotukset.....	33
7.4 Oman oppimisen arviointi.....	33
Lähteet	35
Liitteet.....	39
Liite 1. Kyselylomake.....	39

1 Johdanto

Internet kehittyvä vähitellen ja me emme huomaa monia pieniä muutoksia, kunnes ymmärrämme yhtäkkiä, että Wikipediasta on tullut tärkein tietolähde, että me kommunikoimme pikaviestien avulla ja emme säilytä asiakirjoja tietokoneessa, vaan pilvisessä varastossa. Alamme käyttämään jotain työkalua, koska se on mielenkiintoista ja lupaa jotain uutta, siitä tulee osa jokapäiväistä elämäämme. Jossain vaiheessa rahat ovat muuttuneet "digitaaliseksi". Ne kehittyivät ja tunkeutuivat internetiin syvemmälle, kunnes ilmestyivät täysin virtuaalimuodossa, nimittäin kryptovaluuttana. Internet-palvelujen tavoin kryptovaluutat ovat yleistyneet. Joka päivä ilmestyy uusia kryptovaluuttoja, kryptopalveluja ja niihin liittyviä markkinoita. Kryptovaluuttojen ympärillä niiden kymmenen vuoden olemassaoloaikana on muodostunut terve infrastruktuuri, jonka osa on kryptovaluuttojen louhinta, jota tukee kryptoyhteisö.

Kryptovaluutan hankintaprosessi ei ole jonkinlainen viihde, vaan se on melko vakava ja vastuullinen työ, joka vaatii paljon fyysisiä ja aineellisia panoksia. Kaivostoiminta edellyttää huolellista valmistelua: tarvittavien laitteiden ja ohjelmistojen olemassaolo, optimaalisen tuotannon valinta, hankinnan budjetin suunnittelu tai kapasiteetin lisääminen sekä työn lopullisten tavoitteiden määrittely.

Tässä opinnäytetyössä tarkastellaan kaivostoimintaa kuin ilmiötä ja käsitellään siihen liittyvää ekosysteemiä, kuten useimmissa kirjoissa, artikkeleissa ja uutisissa sanotaan pääosin kryptovaluutasta, mutta kryptovaluutan liikkeeseenlaskun prosessia julkisessa lohkoketjuverkossa ei ole otettu riittävästi huomioon. Opinnäytetyön pääosa koostuu tietoperustasta, empiirisestä osasta sekä loppupohdinnoista. Teoreettisessa osassa käsitellään louhintatoiminnan (eli kaivostoiminnan) ekosysteemin elementtejä, kuten: lohkoketju ja kryptovaluutta, kaivostoiminnan laitteisto ja ohjelmisto, infrastruktuuri. Tämä tieto on edellytys sille, että muodostuu käsitys kaivostoiminnasta kuin prosessista. Tämän työn empiirisessä osassa esitetään kyselyn tutkimustulokset, tämä kysely järjestettiin kaivostoimintaan liittyvien ihmisten kesken, jotka ovat myös suurimpien yhtiöiden jäseniä sellaisilla Internet-paikoilla, kuten Internet-foorumit, sosiaalisten verkostojen ryhmät ja YouTube:n kanavat. Tämän kyselyn päätavoitteena on löytää tehokkaita välineitä kryptovaluuttojen kaivostoimintaa varten ottaen huomioon yhteisön mielipiteen.

Tämän työn viimeisessä osassa tai loppupohdinnassa tehdään päätelmät tutkimuksen pohjalta optimaalisesta kaivoslaitteistosta ja laitteiden ominaisuuksista.

Tämän opinnäytetyön tavoitteena ei ole positiivisen tai negatiivisen mielipiteen muodostaminen kryptovaluuttojen louhinnasta. Tässä opinnäytetyössä ei arvioida kryptovaluuttojen

louhintaan liittyviä riskejä. Kuten esimerkiksi lainsäädännön ja sääntelyn muutokset, markkinamuutokset (volatiliteetti, kilpailun kiristyminen), teknologiset (kvanttietokoneet), turvallisuusriskit.

Suoritetusta tutkimuksesta saadut tulokset ja tehdyt johtopäätökset saattavat olla vain suositusluonteisia, koska tämän opinnäytetyön tarkoitus ei ole laboratoriotutkimuksen tulosten vahvistaminen.

2 Perusteknologia

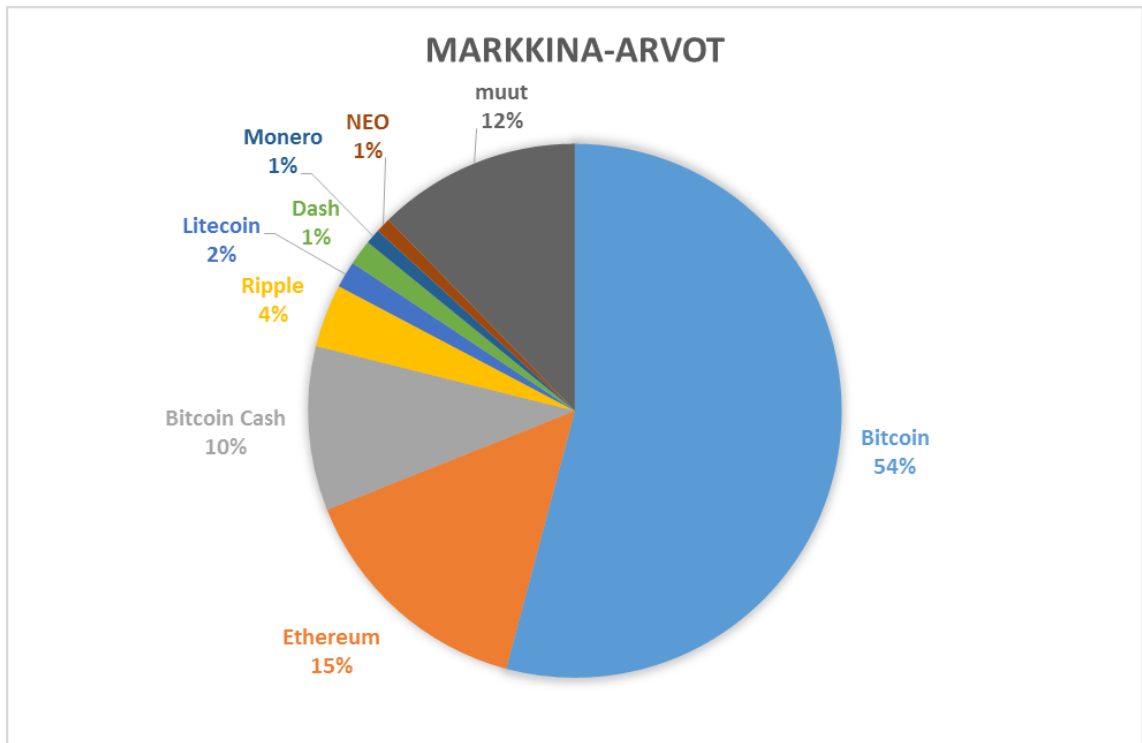
On tärkeää ymmärtää, että minkä tahansa nykyaikaisen kryptovaluuttajärjestelmän yleinen rakenne muodostuu kolmesta tasosta: lohkoketju, protokolla, valuutta. Tämän järjestelmän pohjataso on lohkoketju – julkinen hajautettu rekisteri, joka sisältää tietoja transaktioista ja jota käyttävät kaikki verkkosolmut. Keskimäinen taso on protokolla - ohjelmapaketti, joka siirtää varoja tallentamalla transaktioita lohkoketjuun. Järjestelmän ylätaso on valuutta. Jokainen kolikko on samanaikaisesti valuutta ja protokolla, se voi käyttää omaa lohkoketjuaan tai muun valuutan lohkoketjua. Näitä käsitteitä käsitellään yksityiskohtaisemmin jäljempänä. (Swan 2017, 21–22.).

2.1 Kryptovaluutta

Kryptovaluutta on digitaalinen (virtuaalinen) valuutta, jonka yksikkö on kolikko. Kolikko on suojattu väärentämiseltä, koska se on salattu tieto, jota ei voi kopioida tällä hetkellä (Wikipedia 2017a).

Ennen lohkoketjun kryptografian syntyä digitaalinen käteisraha, kuten mikä tahansa muu digitaalinen omaisuus, voitaisiin kopioida loputtomasti. Tällöin oli mahdotonta ilman erikoisvälittäjää vahvistaa, onko digitaalista rahaa käytetty vain kerran. Bitcoin on ensimmäinen ratkaisu digitaalista rahaa koskevaan pitkäaikaiseen ongelmaan eli kaksinkertaisen käytön ongelmaan yhdistämällä vertaisverkko-teknologiaa ja julkisen avaimen salausta. Nyt kolikoiden omistusoikeus on rekisteröity julkiseen päiväkirjaan, sen vahvistavat kryptografinen protokolla ja louhijoiden yhteisö. Kun tätä teknologiaa käytetään transaktion suorituksen aikana, käyttäjän ei tarvitse luottaa vastineeseen tai välittäjään, mutta on vain luotettava järjestelmään – lohkoketjun protokollan ohjelmistototeutukseen. (Swan 2017, 23.).

Tällä hetkellä (marraskuu 2017) coinmarketcap.com:n (2017a) mukaan on olemassa 1278 kryptovaluuttaa, jotka eroavat kustannuksista, hajautusalgoritmista, louhinnan monimutkaisuudesta, hyökkäyskestävyydestä, transaktioiden vaadittujen vahvistusten määrästä, energiakustannuksista, provision määrästä, hajautusnopeudesta (hash:ien määrä sekunnissa), nopeudesta jne. Kryptovaluuttojen markkina-arvo on 204 miljardia, Bitcoinin osuus on 54 %. Kuviosta näkyy kolikoita, joilla on suurin markkina-arvo, jota tukee teknologia ja käyttäjien luottamus (Kuvio 1).



Kuvio 1. Kryptovaluuttojen markkina-arvot (coinmarketcap.com)

Kryptovaluuttojen ominaisuuksia ja piirteitä analysoimalla voi korostaa tärkeimpiä eroja tavanomaisiin perinteisiin valuuttoihin verrattuna. Positiivisia piirteitä ovat transaktioiden anonymiteetti, vertaisverkko, yhtenäisen digitaalipankin puute, transaktioiden ja maksujen valvonnan puute, avoin algoritmikoodi, kopiosuojaus. On myös ongelmallisia paikkoja: sähkölompakon salasanan menettäminen tai lompakon toimintahäiriö voi johtaa kaikkien siellä olevien varojen peruuttamattomaan menettämiseen, mahdolliset negatiiviset toimet kryptovaluuttoihin nähden kansallisten sääntelyviranomaisten puolelta, korkea volatiliiteetti, vaikeustaso tai suuret sähkökustannukset voivat tehdä louhintatoiminnan kannattamattomaksi.

2.2 Lohkoketju

Melanie Swan antaa kirjassaan Blockchain: Blueprint for a New Economy seuraavan määritelmän teknologian perustasolle. Lohkoketju on teknologia, jonka avulla toimii turvallinen hajautettu tietojen tallennus kaikista transaktioista, jotka on koskaan tehty. Se on tietolohkojen ketju, jonka volyymi kasvaa jatkuvasti, kun louhijat lisäävät uusia datalohkoja viimeisimmistä transaktioista, Bitcoin-verkossa suoritetaan tallennus 10 minuutin välein. Lohkot tallennetaan lohkoketjuun lineaarisessa peräkkäin-aikajärjestyksessä. Jokaiseen täyteen solmuun (tietokoneeseen), joka on liitetty verkkoon asiakkaan avulla, joka suorittaa transaktioiden tarkastukset ja siirrot, tallennetaan kopio lohkoketjusta, joka latautuu automaattisesti, kun louhija liittyy verkkolohkoon. Rekisterissä säilytetään täydelliset tiedot

kaikista osoitteista ja saldoista ensimmäisestä lohkokosta lähtien viimeiseen lisättyyn lohkoon asti. (Swan 2017, 13.).

Melanie Swan työssään ehdottaa jakaa lohkoketjut kolmeen sukupolveen, riippuen kehitystasosta. Lohkoketjun ensimmäiseen sukupolveen "Blockchain 1.0" kuuluvat virtuaaliset valuutat (kryptovaluutat), joista ensimmäinen oli bitcoin. Toinen sukupolvi on ns. "älykäs sopimus" (Smart contract). "Smart contract" on digitaalinen protokolla, joka suorittaa automaattisesti ennalta määritetyt transaktioprosessit ja ei vaadi kolmannen osapuolen (esimerkiksi pankin) osallistumista. Melanie Swan:in listan viimeinen sukupolvi -"Blockchain 3.0"- on nykyään vain konseptin muodossa. "Blockchain 3.0" on teknologian kehitysvaihe, joka perustuu "älykkään sopimuksen" käsitteeseen, mutta tulevaisuudessa osapuolet ovat hajautettuja, itsenäisiä organisaatioyksiköitä, jotka noudattavat omia lakeja ja toimivat käytännössä itsenäisesti. (Swan 2017, 11, 28, 45–46)

Blockchain-teknologian tärkeimmät edut ovat avoimuus ja turvallisuus. Avoimuus on teknologian yksi tärkeimmistä säännöistä. Kaikki lohkojen tiedot ovat aina avoimia kaikille. Ne on helppo tarkistaa, kaikkia tietojen muutoksia on helppo seurata. Siksi todentaminen on yksinkertaista ja helppopääsyistä. Esimerkiksi blockchain.info-sivustolta voidaan saada tarvittavia tietoja transaktioista, lompakosta, lohkokosta tai Bitcoin-verkon tilastoista.

Turvallisuus perustuu konsensus- ja hajautusalgoritmeihin. Kaksi tunnetumpaa konsensusalgoritmia ovat Proof-of-Work ja Proof-of-Stake. Proof-of-Work -mekanismi takaa verkon solmun kyvyn tarkistaa, että louhija (tässä roolissa toimii solmu, joka lisää uuden lohkon lohkoketjuun) on tosiallisesti suorittanut laskelmat. Tässä prosessissa yritetään löytää lohkon otsikon hash:in (lohkon osa, joka sisältää linkin edelliseen lohkoon ja siihen sisältyvien transaktioiden yhteenlasketun arvon), joka vastaa nykyistä vaikeustasoa. Bitcoin-verkkoon sovellettu Proof-of-Work -algoritmi on aiheuttanut ns. louhintateollisuuden muodostumista ja antanut sysäyksen erikoislaitteiden kehittämiseksi, koska laskentaresurssit, joita käytetään lohkojen hajautukseen, ovat erittäin suuria ja ylittävät selvästi suurimpien supertietokoneiden kapasiteetit. Konsensuksen vaihtoehtoinen mekanismi, joka toteutettiin ensimmäisen kerran 2012 kryptovaluutassa PPCoin, on Proof-of-Stake. Myös Proof-of-Stake -algoritmin lähestymistavan mukaan solmut yrittävät hajauttaa tietoa tulosta etsimässä, mutta tässä tapauksessa monimutkaisuus jaetaan verrannollisesti ja riippuen solmun taseen suuruudesta. Toisin sanoen käyttäjän tilillä olevien kolikkojen määrän mukaan. Siten on enemmän mahdollisuuksia luoda seuraavan lohkon solmulla, jonka tase on suurempi. (BitFury Group 2015).

Hajautusalgoritmi on tarpeen, jotta voidaan muuttaa minkä tahansa pituiset syöttötiedot bittiseksi eli määräkokoiseksi ulostuloriviksi. Hajautusfunktio antaa määritetylle tietosarjalle yhden hash:in, jolla on kaksi erittäin tärkeätä ominaisuutta. Ensimmäinen on se, että vaikka jollakin olisi avain, ei voi hän saada tietää, millainen oli alkuperäinen tietosarja ja toinen on se, että on lähes mahdotonta löytää toista tietosarjaa, joka antaa saman hash:in. Maailman ensimmäisen kryptovaluutan perusta on SHA-256-algoritmi. Teknisesti SHA-256-algoritmi toimii seuraavasti: alkuperäinen viesti jaetaan lohkoihin ja jokainen lohko jaetaan 16 sanaan. Jokainen viestilohko kulkee läpi algoritmin syklin, jossa on 64 tai 80 kierrosta. Jokaisen lohkon käsittelyn tulokset lasketaan yhteen, tuloksena oleva summa on hajautusfunktion arvo. (Blockgeeks 2017a).

Tämän algoritmin luomisen jälkeen ei ole alan kehitys päättynyt, joka vuosi ohjelmoijat keksivät jotain uutta. Tällä hetkellä on olemassa monia hajautusalgoritmeja: SHA-256, Ethash, CryptoNight, Equihash, NeoScrypt, X11Gost, Pascal, Blake (14r), Groestl, Scrypt, Qubit, X11, Quark jne. (Whattomine 2017a, Whattomine 2017b). Näiden päätarkoituksena on estää erikoislaitteiden kehittämisen louhintatoiminnan alalla ja yrittää sen avulla välttää keskittämistä.

3 Kryptovaluutan louhintalaitteisto

Alussa kryptovaluutan louhintalaitteisto oli tavallinen henkilökohtainen kotitietokone, joka käyttää prosessorin kykyä matemaattisten ongelmien ratkaisemiseksi, jotka varmistavat kryptovaluutan tuottamisen. Tällä tavoin ilmestyi ensimmäinen ja suosituin Bitcoin-kryptovaluutta. Alan kehittämisen alkuvaiheessa tavanomaisen henkilökohtaisen tietokoneen kapasiteetti oli riittävä tarvittavan datamäärän käsittelemiseen, mutta liikkeeseen lasketun valuutan määrä kasvoi ja uusien lohkojen tallentaminen vaati suuria ponnistuksia, mikä johti siihen, että uusien kolikoiden luomisen nopeus hidastui jopa tehokkaimmissa tietokoneissa. Yksinkertaisesti sanottuna, yhden kolikon hankintakustannukset alkoivat ylittää sen hinnan. Tällä hetkellä (syyskuu 2017) kryptovaluutasta riippuen ovat taloudellisesti tarkoituksenmukaisia kaksi laitteen tyyppiä: ASIC (Application Specific Integrated Circuit, sovelluskohtainen mikropiiri) louhintalaitteisto ja GPU (Graphic Processing Unit, grafiikkaprosessori) louhintalaitteisto. (Newsbtc 2016).

3.1 ASIC louhintalaitteisto

ASIC (Application Specific Integrated Circuit, sovelluskohtainen mikropiiri) on mikropiiri, joka on suunniteltu ratkaisemaan tiettyjä ongelmia. Toisin kuin yleiskäyttöiset mikropiirit, erikoissiruja käytetään tietyssä laitteessa ja ne suorittavat tiukasti rajoitettuja toimintoja, jotka ovat ominaisia vain tälle laitteelle. Niitä käytetään ASIC-louhintatoimintaa varten, koska tiukasti määritellyn rakenteen ansiosta mikropiirien valmistusprosessi tulee paljon halvemmaksi ja sirujen kapea-alaisen erikoistumisen ansiosta lisääntyvät tuottavuus ja energiatehokkuus. (Bitcoin Wiki 2015a).

ASIC louhintatoiminnalle ovat ominaisia seuraavat erikoisominaisuudet: yksinkertainen asetus, pieni määrä komponentteja työn varmistamiseksi (virtalähde ja verkkokaapeli), toimivat vain rajoitetulla määrällä algoritmeja (SHA-256, Scrypt, X11, Quark, Qubit) (Whattomine 2017b), korkea melutaso, korjaus on lähes mahdotonta, mallien nopea vanheneminen.

Tämän alan kiistaton johtaja on kiinalainen yritys Bitmain Technologies Limited. Crypto-compare.com-sivuston (2017a) mukaan, viisi tehokkainta louhintalaitetta ovat D3 Antminer ASIC, S9 Antminer ASIC, L3 + Antminer ASIC, T9 Antminer ASIC ja Antminer R4 ASIC, valmistaja Bitmain Technologies Limited.

3.2 GPU louhintalaite

GPU louhintalaite on pohjimmiltaan sama henkilökohtainen tietokone, jolla on vain enemmän videokortteja, kaksi tai useampia. Soveltuu sekä aloitteleville käyttäjille että ammattilaisille. Konseptin avulla voidaan konfiguroida käyttäjän tarpeiden mukaisen laitteiston. Käyttöala rajoittuu krypto-valuuttoihin, joita ei tuoteta erikoislaitteissa (ASIC), koska ASIC-laitteiden kehitys on mahdotonta tai taloudellisesti epätarkoituksenmukaista.

Tämän tyyppisillä laitteilla on seuraavat ominaisuudet: alhainen melutaso, korjattavuus, tekninen kyky tuottaa kaikenlaisia valuttoja, merkittävä jäännösarvo, vaativat aikaa asennusta ja kokoonpanoa varten, tiheämmät huoltovälit. Järjestelmän pääosa, joka tarjoaa laskelmia, on grafiikkaprosessori. Tärkeimpiä valmistajia ovat AMD ja Nvidia. NiceHash: n kannattavuuden laskimen mukaan seuraavat tuotesarjat ovat tehokkaimpia: Nvidia GTX 1080 Ti, GTX 1080, GTX 1070, GTX 1060 ja AMD RX 470, RX 480, RX 570, RX 580, RX VEGA. (Nicehash 2017a).

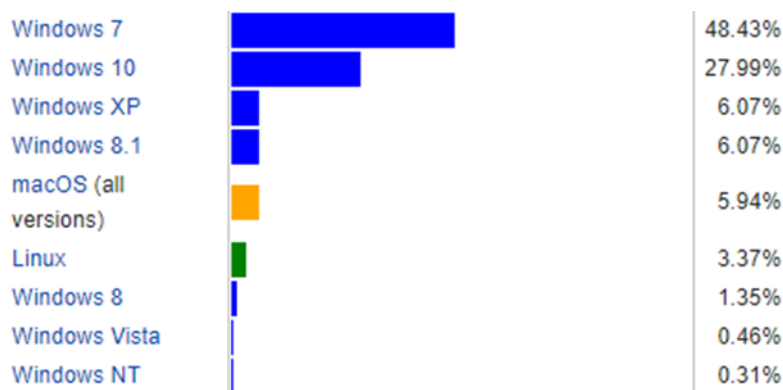
4 Ohjelmisto louhintatoimintaa varten

Ohjelmiston oikea valinta on erittäin tärkeää laadullisen ja tehokkaan työn kannalta. Ohjelmiston tehtävänä on pohjimmiltaan muodostaa yhteyden lohkoketjuun tai kaivosaltaaseen sekä siirtää kaivoslaitteiston tekemä työ muihin verkko-osiin ja saada valmiit työt muilta louhijoilta. Lisäksi ohjelmiston avulla voidaan seurata tärkeitä tilastoja, kuten louhintatoiminnan nopeutta, hajautusta ja lämpötilaa.

4.1 Klassiset käyttöjärjestelmät

Wikipedia (2017b) antaa seuraavan määritelmän tietokoneen käyttöjärjestelmälle. Käyttöjärjestelmä - joukko ohjelmia, jotka varmistavat tietokoneen laitteiston hallinnan, järjestää tiedostojen työtä ja sovellusohjelmien suorittamista, sovellusohjelmat suorittavat tietojen syöttämisen ja ulostulon. Useimmissa tietokoneissa käyttöjärjestelmä on järjestelmäohjelmiston tärkein (ja joskus ainoa) osa.

Netmarketshare.com:in (2017a) mukaan noin 90% henkilökohtaisten tietokoneiden käyttäjistä käyttää eri versioita Windows-käyttöjärjestelmästä, noin 6% macOS:ista ja 3% Linux:ista (Kuvio2).



Kuvio 2. Desktop OS:in markkinaosuus NetMarketShare:n mukaan elokuussa 2017

Kaikki yllä mainitut käyttöjärjestelmät tarjoavat enemmän tai vähemmän mahdollisuuden kryptovaluuttojen louhinnan toimintaan. Mielenkiintoisimpia ovat kaksi käyttöjärjestelmää: Windows ja Linux, koska pääohjelmistoja kehitetään juuri niitä varten ja useimmilla käyttäjillä on kokemusta niiden käytöstä.

Perustuen keskustelun analyysiin aiheesta „Linux vs. Windows louhintatoiminnan alalla“, josta keskustelivat eri temaattisten foorumien käyttäjät, on mahdollista tuoda esiin niiden käyttöjärjestelmien edut ja haitat. Käsittelemme niitä edelleen. (Bitcointalk 2014a; Ethereum Community Forum 2017; Miningclub.info 2017).

4.1.1 Microsoft Windows

Tällä hetkellä (syyskuu 2017) käyttöjärjestelmän viimeisin versio on Windows 10. Käyttöjärjestelmän asennus ei eroa edellisistä versioista ja kestää noin 1 tunti. Asennuksen jälkeen käyttöjärjestelmä vaatii konfiguraatioita, kuten: rekisterissä palveluiden poistaminen käytöstä, jos niitä ei käytetä louhintatoiminnassa (suositus), Windows:in päivitysten poistaminen käytöstä, virtuaalimuistin lisääminen 16 GB: iin, virransäästöasetusten muuttaminen ja ohjainten päivittäminen. Kaikki nämä toimet kestävät 10–20 minuuttia. Ja kaikkien tarvittavien asetusten jälkeen järjestelmä saattaa pysyä epävakaisena ja vaatia seuranta. Windows 10 Home järjestelmän käyttöoikeuden hinta on 119,99 USA:n dollaria. Windows-käyttöjärjestelmän ainutlaatuiset edut ovat helppokäyttöisyys, mahdollisuus automatisoida kaivosprosessi ilman ohjelmakoodia ja myös laaja valikoima ohjelmistoja laitteiden valvontaan ja niiden työn optimointiin.

4.1.2 Linux-pohjaiset käyttöjärjestelmät

Wikipediasta (2017c) voi löytää seuraavan määritelmän: ”Arkikielessä Linuxilla tarkoitetaan usein kokonaista käyttöjärjestelmää, jonka ytimenä Linux toimii, eli Linux-jakelua, joka sisältää ytimen lisäksi muun muassa erilaisia kirjastoja, apuohjelmia, käyttöliittymiä ja sovelluksia valmiiksi paketoituna loppukäyttäjää varten, helpottamaan tietokoneen käyttöönottoa”.

Voi tuoda esiin useita käyttöjärjestelmiä, jotka perustuvat Linux-lähdekoodiin, jotka käyttäjät ovat useimmin asentaneet, kuten Ubuntu, Linux Mint, Fedora, Debian, Deepin. Kaikilla niillä on samat ominaisuudet, joiden perusteella voidaan puhua eduista ja haitoista.

Linux-lähdekoodiin perustuvien käyttöjärjestelmien edut ovat seuraavat: asennuksen nopeus, asennus kestää normaalioloissa 15–30 minuuttia. Asennuksen jälkeen käyttäjän on päivitettävä ohjaimet ja asennettava SDK / CUDA-työkalupakki. Käyttäjien käytäntö osoittaa, että järjestelmä pysyy vakaana jopa monimutkaisemmissa kokoonpanoissa. Käyttöjärjestelmät ovat ilmaisia tai shareware (maksulliset julkisohjelmat). Linux-lähdekoodiin perustuvien käyttöjärjestelmien miinus on monimutkaisuus taitamattomalle käyttäjälle, siihen kuuluvat vähemmän intuitiivinen käyttöliittymä, tarve työskennellä CLI: n (komentorivirajapinnan) kanssa, ohjelmakoodin automaatioasetukset ja pieni ohjelmistojen valikoima laitteiden työn ohjaukseen ja optimointiin. (Steemit 2017)

4.2 Käyttöjärjestelmät louhintatoiminta varten

Käyttöjärjestelmien päätehtävä, josta keskustellaan myöhemmin, on kryptovaluutan kaivos- eli louhintatoiminta. Nämä käyttöjärjestelmät on suunniteltu sekä tavallisille käyttäjille, jotka haluavat tuottaa tai tuottavat kryptovaluuttaa, sekä ammattilaisille, koska pohjimmitaan nämä käyttöjärjestelmät on rakennettu Linux: ille.

Louhintatoiminnan käyttöjärjestelmät mahdollistavat nopeasti lisää kapasiteettia ja sisältävät myös perustoiminnot laitteiston, ohjainten, louhintaohjelmistojen ja kaukohallintaohjelmistojen toimintaan. Bitcointalk.org-foorumissa käynyt keskustelun ja avoimilla lähteillä olevien tietojen analyysin perusteella voidaan erottaa useita käyttöjärjestelmiä, joilla on testattu ratkaisu ja kehittäjän tuki: SimpleMining OS, ethOS, PiMP OS.

4.2.1 Käyttöjärjestelmä ethOS

Linux-ytimeen perustuva 64-bittinen käyttöjärjestelmä mahdollistaa Ethereumin, ZCashin, Moneron ja jonkin muun kryptovaluutan ottamisen. On olemassa funktionaalinen automaattinen valuuttavaihto Altcoin-Bitcoin. Käyttöjärjestelmän asennuksen jälkeen, se tunnistaa automaattisesti laitteiston kokoonpanon ja asentaa tarvittavat ohjelmistot. Käyttäjän on määritettävä vain kaivostoiminnan allas. Käyttöjärjestelmällä on ystävällinen käyttöliittymä etäohjaukseen, laitteiston seuranta, järjestelmä on erittäin helppo asentaa. Tämän käyttöjärjestelmän etu on se, että on mahdollista työskennellä yli kahdeksan näytönohjaimen kanssa, kun taas Windows rajoittaa samanaikaisesti käytettyjen näytönohjaimien määrää kahdeksalla kappaleella. Yhden lisenssin hinta on 39 USA:n dollaria. 26.09.2017 datan mukaan tätä käyttöjärjestelmää käyttävät 32664 kaivostoiminnan laitetta. Uusin julkaisu ethOS 1.2.5 15.9.2017. (ethOS 2017).

4.2.2 Käyttöjärjestelmä PiMP OS (Portable Instant Mining Platform)

Erittäin yleinen 64-bittinen käyttöjärjestelmä, joka perustuu Linux-ytimeen. Tukee kaikkia yleisiä näytönohjaimia, joita käytetään louhintatoiminnassa, tietoruudun tuki, louhintatoiminnassa käytettävät seurantalaitteet miner.farm, yksinkertaiset ohjauskomennot, diagnostiikka ja enemmän. Lisäksi kehittäjät väittävät, että tämä käyttöjärjestelmä voi parantaa tuotannon kannattavuutta. Käyttäjä toimii pääasiassa web-sovelluksen min.farmin kanssa laitteiden valvontaan ja ohjaukseen. On syytä kiinnittää huomiota siihen, että PiMP-käyttöjärjestelmä ei tue USB-aseimia, käyttäjillä pitäisi olla kiintolevy tai SSD. PiMP-käyttöjärjestelmä maksaa 30 USA:n dollaria yhdelle lisenssille. Verkkosivuston mukaan GetPimp on ladattu yli 136 000 kertaa ja sillä on 2 544 aktiivista käyttäjää. Uusin versio PiMP OS PIMP 2.1 6.6.2017. (PiMP OS 2017).

4.2.3 Käyttöjärjestelmä SimpleMining OS

Käyttöjärjestelmä SimpleMining perustuu Linux:in lähdekoodiin ja on suunniteltu Altcoin-kryptovaluutan louhintatoimintaan. Käyttöjärjestelmä sisältää kaivosprosessin seurantajärjestelmän, joka perustuu web-käyttöliittymään, sen avulla voidaan hallita kaivosprosessia suoraan projektisivustolta ilman sitä, että tulee asentaa lisäohjelma etäohjaukseen. Ohjauspaneelin kautta toteutetaan tukea videokorttien suorituskyvyn parantamiseen, mutta tässä tapauksessa on oltava tarkkana asetuksia kohtaan, koska virheelliset asetukset voivat aiheuttaa laitteiden vaurioita. Tällä hetkellä työtä varten SimpleMining-käyttöjärjestelmän kanssa tarvitaan vähintään 8 Gt: n USB-tallennuslaite. Käyttöjärjestelmän käytön aloittamiseen tarvitsee vain syöttää käyttäjätunnus (e-mail) ja päästä projektin verkkosivuille sekä tehdä kaivosohjelmiston asetukset. SimpleMining OS on shareware, maksu veloitetaan vain todellisesta käytöstä 2 USA: n dollaria per kaivoslaitteiston yksikkö. (SimpleMining 2017).

4.3 Louhinnan asiakasohjelmat

Tällä hetkellä on olemassa lukuisia erikoisohjelmistoja kaivoslaitteiston liittämiseen lohko-ketjun verkkoon ja työn suorittamiseen. Suurin osa ohjelmistosta on ilmainen tai shareware, mikä laajentaa mahdollisuuksia. Ohjelmistoa valittaessa seuraavat tekijät ovat tärkeitä: kaivoslaitteisto (CPU, GPU, ASIC), tuotettava valuutta ja mahdollisuus tehdä asetuksia nykyiset tehtävät huomioon ottaen.

On olemassa useita ohjelmatyyppejä, joilla on samanlaiset asetukset. Monia valuu-toja varten käytetään erityisohjelmia, jotka voidaan ladata projektin verkkosivustolta. Esimerkiksi ethereumia varten käytetään ethminer. Ohjelma liitetään altaan palvelimen osoitteen läpi tietokoneeseen ja aloitetaan prosessi. Useimmissa tapauksissa ohjelman kuoressa on konsolinäkymä, jossa on tekstitietoja prosessinopeudesta, lämpötilasta, nykyisestä löydetystä lohkoista ja prosessin tilasta. Suosituimpia ohjelmistojen tuottajia Altcoin-valuutan kaivostuotantoa varten ovat Claymore ja Genoil, Bitcoin, CGminer, BFGMiner.

Claymore's DualMiner toimii useimpien nykyaikaisten näytönohjainten kanssa, mahdollistaa kolikoiden tuotannon, jotka perustuvat Dagger Hashimoto: n (Ethereum, Ethereum Classic, Expandse, Ubiq jne.) sekä Decred, Siacoin, Lbry, Pascal algoritmeihin. Kaksoistuotantotilalla (kaksinkertainen kaivostoiminta) voit tuottaa samanaikaisesti kahta eri valuuttaa ilman huomattavaa nopeuden menetystä verrattuna yhden valuutan tuotantoon ("yksinlouhinta"). Käyttäjille tarjotaan vaikuttava joukko erilaisia asetuksia sekä verkkopalvelinta etävalvontaan ja hallintaan. (Bitcointalk 2017a).

Nykyään CGMiner on yksi suosituimmista ohjelmista, joka soveltuu GPU / FPGA / ASIC open source-kaivostoimintaan. Se soveltuu Windows, Linux ja OS X: lle. Ohjelmiston toiminnot sisältävät valvonnan, mahdollisuuden asettaa etäliitännän, puhaltimien ohjauksen, prosessorien ja grafiikkaprosessorien näytönohjainten älyllisen analyysin. (Bitcointalk 2017b).

4.4 Ohjelmisto optimointiin ja mukauttamiseen

Laitteiston mukauttamisen aikana on yksi tehtävistä laskunopeuden ja vakauden lisääminen, mikä ilmaistaan laitteiston ominaisuuksien voimakkaalla lisääntymisellä. Näytönohjaimen tapauksessa sen teho riippuu suoraan kahdesta parametrasta: GPU: n kellotaajuudesta ja videomuistin kellotaajuudesta. Ehdollisesti voidaan jakaa optimointiprosessi kolmeen vaiheeseen: taajuuden lisääminen, järjestelmän tarkistus stressitestissä ja stabiiliuden tarkistus suoraan kaivosalueella. Ohjelmistopaketti on seuraava: näytönohjaimen optimointiohjelma (MSI Afterburner, Radeon WattMan, EVGA Precision jne.), ohjelma videokortin kaikkien parametrien seuranta varten (GPU-Z, NVIDIA Inspector jne.) ja ohjelmat suorituskyvyn testaamiseksi (3DMark, Furmark jne.). Kun käytät AMD-valmistajan grafiikkaprosessoreita, joissakin tapauksissa on tarpeen tehdä muutoksia näytönohjaimen BIOSin optimointiin. Tätä varten käytetään kirjoittamisen / lukemisen ohjelmaa ATiWin-flash ja Polaris Bios Editorin käytetään muokkaamiseen.

5 Infrastrukturi

5.1 Kaivosallas

Louhinta- eli kaivostoiminnalla tai lohkon allekirjoituksen valinnan prosessilla on suuri laskennallinen vaikeus. Se on yksi tärkeimmistä parametreista louhijaa varten, koska vaikeuden muutoksesta riippuu kannattavuus. Kunnes verkkojen monimutkaisuus oli vähäinen, oli olemassa niin sanottu "soolo"-louhinta. Laskennallisen tehtävän ratkaisu voitaisiin suorittaa jopa yhdellä tietokoneprosessorilla, joten jokainen louhija työskenteli yksin ja sai itse korvauksen. Monimutkaisuuden kasvun myötä soolo-louhinta on jäänyt menneisyyteen. Esimerkiksi Bitcoin-verkostossa, jopa tehokkaimpien erikoisvarusteiden avulla voi työskennellä useita vuosia, mutta hash:ia lohkon allekirjoittamista varten ei löydy - tarvitaan satoja tällaisia laitteita. Siksi, kun kryptovaluutat ovat saavuttaneet suosiota, on syntynyt yhteinen kaivostoiminnan teknologia - useiden itsenäisten louhijoiden yhdistäminen kaivosaltauksiin (Pool mining 2017). Kaivosaltaan valinta riippuu monista tekijöistä ja useimmissa tapauksissa on yksilöllistä. Käyttäjän on kiinnitettävä huomiota seuraaviin ominaisuuksiin: sivuston käyttöliittymä, komissio, palkitsemisjärjestelmä, automaattinen peruuttaminen ja bitcoineiksi vaihto haluttaessa, tuettavat kryptovaluutat, maksujen oikea-aikaisuus, laitteiston todellisen nopeuden vastaavuus, yksityiskohtaiset tilastot, palvelimen sijainti ja käyttäjien määrä.

Kaivosallas on palvelin, joka jakaa lohkon allekirjoituksen laskentatehtävän kaikkien liitettyjen osallistujien kesken. Jokaisen osallistujan panos arvioidaan käyttäen niin sanottua "osaketta", joka on potentiaalinen ehdokas allekirjoituksen saamiseksi. Heti kun joku "osake" osuu kohteeseen, allas ilmoittaa lohkon valmiudesta ja jakaa palkkioita. Pienen kapasiteetin omaava louhija voi työskennellä hyvin pitkään, ei löydä yhtä lohkoa, mutta saa osuutensa. Maksu suoritetaan sen todennäköisyyden perusteella, että yksi hänen ratkaisuisistaan on oikein.

Jokaisella altaalla on omat säännöt ja maksutavat. Allas saa osuutensa suoritetusta palvelusta ja maksaa louhijoille palkkion käyttäen yhtä monista järjestelmistä. Tärkeimpiä maksujärjestelmiä käsitellään edelleen.

PROP (Proportional) - suhteellinen malli, jossa lohkon palkkio jaetaan tiukasti suhteessa jokaisen louhijan lähettämään osuuteen. Kun lohko on löydetty, vastaanotettujen "share" laskuri nollataan ja laskenta alkaa nollasta. Tämä on yksinkertaisin järjestelmä, mutta maksut ovat erittäin epävakaita.

PPLNS (Pay Per Last N Osakkeet) on myös suhteellinen jakelu, mutta tasaisempi kuin PROP. Maksu lasketaan "share" määrästä, joka ei ole lähetetty kahden löydetyn lohkon

välisenä aikana, vaan sen ajanjakson aikana, joka sisältää kiinteän määrän määriteltyjä aikavälejä.

PPS (Pay Per Share) - kiinteä maksu jokaisesta altaan vastaanottamasta "share":sta. Tässä tapauksessa allas määrittää kiinteän palkkion "share":sta. Käyttäjän näkökulmasta tällainen järjestelmä on oikeudenmukaisempi, koska kaikista suoritetusta työstä maksetaan palkka työn tuloksesta riippumatta.

SMPPS (Jaettu enimmäispalkka per osake) - Käytetään samaa järjestelmää kuin PPS (Pay Per Share), mutta maksetaan niin paljon kuin on ansaittu. (Bitcoinmining 2016; Bitcoin Wiki 2017a).

Pitkällä aikavälillä samassa altaassa työskentelevälle louhijalle ei ole väliä, mitä maksujärjestelmää käytetään. Vielä tärkeämpää on altaan perimä provisio.

Klassisessa muodossaan allas on palvelin laitteiden yhdistämiseen, jotka suorittavat las-kutoimituksia yhdellä algoritmilla. Mutta ajan mittaan ilmestyi monen kolikon altaita. Niihin altaisiin liittyvät louhijat, jotka haluavat ansaita useita kryptovaluuttoja siirtyen tällä hetkellä kannattavimman valuutan altaaseen. Kaikki siirtämiset suorittaa louhija käsin. Itse asiassa monen kolikon allas eroaa tavallisesta vain siinä, että käyttäjän ei tarvitse ylläpitää useampia tilejä jokaista kryptovaluutaa varten. Seuraavassa kehitysvaiheessa ilmestyivät multialtaat. Niiden tärkein etu on se, että kaivostoiminta siirtyy automaattisesti tällä hetkellä kannattavimman kryptovaluutan tuottamiseen. Tässä tapauksessa otetaan huomioon seuraavat tekijät: monimutkaisuus, kolikon hinta pörssissä ja monet muut tekijät. Multialtaissa voidaan ansaita Altcoin-valuuttoja (altcoin – kaikki kryptovaluutat, paitsi bitcoin) monilla yleisillä hajautusalgoritmeilla. (Cryptocompare.com 2017b).

5.2 Kryptovaluuttojen pörssi

Kryptovaluuttojen pörssi on kaupankäyntialusta, jossa pörssin osallistujat voivat vaihtaa keskenään erilaisia kryptovaluuttoja tai vaihtaa niitä fiat-valuutoiksi. Esimerkiksi Altcoinin osto euroilla, sitten vaihto Bitcoineiksi ja Bitcoinin vaihto dollareiksi ovat kryptovaluuttojen pörssin yksinkertaisimmat kaupankäyntioperaatiot. Ehdollisesti voidaan jakaa pörssit kahteen tyyppiin: kaupankäyntialustat, joissa on mahdollista vaihtaa fiat-valuuttoja ja pörssit, joissa on mahdollista vaihtaa kryptovaluutaa vain toiseksi kryptovaluutaksi. (Investopedia 2017).

Tämän luokituksen lisäksi on olemassa myös yksi tyyppinen jakautuminen kaupankäynnin luonteen perusteella.

Kryptovaluuttojen pörssit, jotka pitävät käyttäjien rahatilejä (osallistuja käy kauppaa pörssin kanssa). Tämän ansiosta voidaan tehdä välittömiä kauppvoja, joilla on alhainen kaupankäyntipalkkio, mutta varojen siirto pörssiin ja pörssistä voi kestää jonkin aikaa, koska on olemassa riski, että kolmas osapuoli estää pörssin pankkitilin käytön.

Kryptovaluuttojen pörssit, jotka eivät pidä käyttäjien rahatilejä (osallistuja käy kauppaa muiden osallistujien kanssa). Niillä on seuraavat ominaisuudet: ei ole täydennys- eikä peruuttamismaksua, varojen välitön siirto pörssiin ja pörssistä, ei ole mahdollista tehdä kauppvoja välittömästi, korkea kaupankäyntipalkkio.

Kryptovaluuttojen pörssit, jotka pitävät rahatilejä ehdollisesti, osittain. On mahdollista tehdä välittömiä kauppvoja ja varojen siirtoja pörssiin ja pörssistä, takaa varojen siirron ja vastaanoton. Niillä on alhainen kaupankäyntipalkkio, ei ole täydennys- eikä peruuttamismaksua. (Blockgeeks 2017b).

Resurssin coinhills.com (2017) mukaan on 109 kaupankäyntialustaa, jotka suorittavat liiketoimia kryptovaluuttoilla, joilla on merkittävä päivittäinen liikevaihto. Lähdetietojen analyysin aikana viidellä kauppapaikalla oli päivittäinen liikevaihto yli 5% eli yhteensä 55% liikevaihdosta 2,3 miljardia USA:n dollaria. Nämä kaupankäyntialustat ovat: bitFlyer, Bitfinex, bithumb, Bittrex, HitBTC.

Kaupankäyntialustan valinta voi riippua useista eri tekijöistä, mutta tärkeimmät kriteerit, joita on otettava huomioon ovat seuraavat: maine, palkkiot, kaupankäyntiparien määrää, likviditeetti, maksuvaihtoehdot, käyttäjien todentamisvaatimukset, kauppapaikan perustana oleva maa, käyttöliittymän helppous, teknisen ja graafisen analyysin välineet, kätävien tilastojen saatavuus. (Coinpursuit 2017).

5.3 Kryptolompakko

Jotta voidaan työskennellä millä tahansa kryptokolikolla, tarvitaan digitaalinen lompakko (crypt-wallet) eli kryptolompakko. Kryptolompakko on ohjelma, joka tallentaa yksityisiä ja julkisia avaimia, on vuorovaikutuksessa lohkoketjun kanssa, jotta käyttäjät voivat lähettää ja vastaanottaa kryptovaluuttoja ja hallita tasettaan (Bitcoin Wiki 2017b). Toisin kuin tavalliset lompakot, kryptolompakot eivät tallenna valuuttaa. Itse asiassa kryptovaluuttaa ei ole fyysisessä muodossa eikä sitä säilytetä yhdessä paikassa. Kaikki, mitä on olemassa, on lohkotiloissa tallennetut transaktioihin liittyvät tiedot.

On olemassa erilaisia kryptolompakon tyyppisiä, jotka tarjoavat erilaisia tapoja tallentaa ja käyttää kryptovaluuttaa. Lompakot voidaan jakaa kolmeen luokkaan: ohjelmistot, laitteistot ja niin sanotut paperiset lompakot.

Ohjelmisto-lompakot ovat kolmessa muodossa: ohjelmat henkilökohtaisille tietokoneille, sovelluksia mobiililaitteille ja online-lompakoita.

PC-ohjelmat asennetaan kiinteään tietokoneeseen tai kannettavaan tietokoneeseen. Lompakko on käytettävissä vain laitteesta, johon se on asennettu. Tämä on yksi turvallisimmista tavoista tallentaa kryptovaluuttaa. Jos tietokone on hakkeroitu tai saanut viruksen, on olemassa varojen menettämisen todennäköisyys.

Sovellukset asennetaan mobiililaitteisiin. Nämä lompakot ovat käteviä, koska ne antavat mahdollisuuden käyttää kryptovaluuttaa missä tahansa paikassa. Yleensä ne ovat hieman yksinkertaisempia kuin PC-ohjelmat, johtuen mobiililaitteiden rajoituksista.

Online-lompakot käynnistetään pilvessä, ne ovat saatavilla mistä tahansa tietokonelaitteesta ja missä tahansa paikassa, jos internet-yhteys on käytettävissä. Tällaiset lompakot tallentavat yksityisiä online-avaimia ja niitä lompakoita kontrolloivat kolmannet osapuolet, mikä tekee niistä haavoittuvaisempia hakkerointiin, hyökkäyksiin ja varkauksiin.

Laitteisto-lompakot eroavat ohjelmisto-lompakoista, koska ne säilyttävät käyttäjän yksityisiä avaimia esimerkiksi USB-laitteessa. Vaikka laitteisto-lompakot suorittavat transaktioita on-line, ne säilytetään offline-tilassa, mikä lisää turvallisuutta. Laitteisto-lompakot voivat olla yhteensopivia useiden verkkorajapintojen kanssa ja tukevat eri valuuttoja. Lisäksi ne yksinkertaistavat transaktioita: käyttäjä yhdistää laitteen mihin tahansa tietokoneeseen, jolla on Internet-yhteys, syöttää PIN-koodin ja suorittaa tarvittavat toimenpiteet.

Paperi-lompakko on asiakirja, joka sisältää kopion yksityisestä avaimesta ja julkisesta avaimesta. Usein asiakirja on QR-koodin muodossa, se antaa mahdollisuuden nopeasti skannata sen ja suorittaa toimia kryptovaluutalla. Tämän tyyppisen lompakon tärkein etu on turvallisuus, koska yksityisiä avaimia ei säilytetä tietokoneessa tai verkossa. Myös asiakirjan fyysinen hallussapito laajentaa käyttömahdollisuuksia. (Blockgeeks 2017b).

6 Tutkimus

Työn empiirisessä osassa käsitellään kyselyn muodossa suoritettujen tutkimusten tuloksia. Tutkimus on kvantitatiivista eli määrällistä. Kyselyn aiheena on kryptovaluuttojen louhinnan ekosysteemi. Tämän kyselyn päätavoitteena on määrittää, mitkä ovat louhijoiden yhteisön edustajien mielestä kryptovaluuttojen kaivostoiminnan tehokkaimmat välineet. Tämän tutkimuksen hypoteesi on: välineet ja myös niiden ominaispiirteet ja ominaisuudet, joiden käyttöprosentti on suurin ja jotka ovat tärkeitä louhijoille, ovat optimaalisia käytettäväksi kaikissa yhtäläisissä olosuhteissa. Tämän hypoteesi on tietämyksen kehittämisen muoto, se on perusteltu olettamus, joka on esitetty tutkittavan kohteen ominaisuuksien selvittämiseksi.

6.1 Tutkimusmenetelmät

Tutkimuksessa hyödynnettiin määrällisiä eli kvantitatiivisia tutkimusmenetelmiä. Kvantitatiiviset tutkimusmenetelmät perustuvat aina tiukkoihin tilastomalleihin, menetelmissä käytetään suuria otantoja. Tämä ei ainoastaan mahdollista mielipiteiden ja oletusten saamista, vaan myös tarkkojen kvantitatiivisten (numeeristen) arvojen löytämistä tutkittaville indikaattoreille. Toisin sanoen kvantitatiivisten tutkimusten tulokset ovat tilastollisesti luotettavia, niitä voidaan soveltaa ryhmään, johon tutkimus on suunnattu. Tutkimukset, joissa hyödynnetään kvantitatiivisia tutkimusmenetelmiä, ovat tärkein työkalu tarvittavien tietojen saamiseksi suunnittelua ja päätöksentekoa varten niissä tapauksissa, kun tarvittavat hypoteesit on jo muodostettu käyttämällä muita (esim. kvalitatiivisia) menetelmiä. Kvantitatiiviset tutkimukset vähentävät riskiä tehdä väärät päätökset ja valita virheelliset suunnittelu-parametrit. (USC 2017).

Heikkilän (2014) mukaan kvantitatiivisen tutkimusprosessin vaiheet ovat:

- Tutkimusongelman määrittäminen
- Aikaisempiin tutkimuksiin ja kirjallisuuteen perehtyminen
- Mahdollisten hypoteesien laadinta
- Tiedonkeruuvälineen rakentaminen (lomakkeen laatiminen)
- Tietojen kerääminen
- Tietojen käsittely ja analysointi
- Tulosten raportointi
- Johtopäätösten teko ja tulosten hyödyntäminen

Tutkimus suoritettiin kyselyn avulla. Kyselylomake on tehty Google:n ohjelmistotuotteen Google Forms:n avulla. Google Forms-ohjelmistoa käytettiin seuraavien kriteerien perusteella: ilmainen käyttö, automaattinen analyysi ja kaavioiden tekeminen, mahdollisuus tuoda saadut tiedot Microsoft Exceliin. Kysely toteutettiin online-kyselylomakkeella, koska verrattuna perinteisiin kyselytyyppeihin, Internetin kautta suoritettavat tutkimukset voivat

säästää huomattavasti aikaa, rahaa ja resursseja. Tärkeä rooli on myös sellaisilla tekijöillä kuten mahdollisuus keskittyä tiettyihin otoksiin ja löytää henkilöitä, joilla on konkreettisia ja erityisiä kiinnostuksia. Osoitetaan, että Internet-kyselytutkimuksissa on tutkijan vaikutusta vastaajan vastauksiin huomattavasti vähemmän kuin perinteisissä kyselyissä. Vastaavasti vähemmän on sosiaalisesti hyväksytyjä, sosiaalisesti toivottavia vastausvaihtoehtoja. Tutkimus sisältää 20 numeroitua kysymystä ja 48 paikkaa vastaajan vastauksille.

Kyselytutkimus toteutettiin lokakuussa 2017 kahden viikon ajan. Vastaajat olivat kryptovaluuttaan liittyviä aiheita käsittelevien Internet-foorumien, sosiaalisten verkostojen ryhmien ja Youtube-kanavien käyttäjiä.

6.2 Kyselylomakkeen rakenne

Tutkimuslomake (kyselylomake) on tärkein kyselytutkimuksen väline ja se on sosiologinen asiakirja, joka sisältää rakenteellisesti järjestetyn joukon kysymyksiä, joista jokainen liittyy tutkimustavoitteisiin. Tämä yhteys ilmenee tarpeena saada tietoa, joka heijastaa tutkittavan kohteen ominaisuuksia (KvantiMOTV 2010). Kyselylomakkeella on tietty rakenne, jossa tärkeät elementit ovat vastaajan ominaisuudet ja pääosa.

Vastaajan ominaisuuksia arvioidaan kysymyksissä 1-5. Kysymykset koskevat vastaajan sosiaali-demografisia ja muita ominaisuuksia. Näiden kysymysten sijainti lomakkeen alussa on perusteltua psykologisesti, koska se mahdollistaa kasvattaa asteittain kysymysten monimutkaisuutta. Kysymykset 1-5 ovat suljettuja, yleisiä, yksinkertaisia sanamuodossa ja vastausvaihtoehtojen valinta ei ole vastaajalle vaikeaa. Kysymyksen sanamuoto sisältää valmiita vastausvaihtoehtoja, joista voidaan valita vain yksi.

Kyselylomakkeen pääosa koostuu kysymyksistä 6-18, jotka liittyvät tutkimuksen tavoitteisiin ja tehtäviin. Kysymykset 6, 8, 10, 12, 13, 15, 17 ovat tärkeimpiä, ne liittyvät suoraan asetettujen tehtävien ratkaisemiseen. Kysymykset 6, 8, 12, 15 ja 17 ovat suljettuja, niiden kysymysten sanamuoto sisältää valmiita vastauksia, joista yksi tai useampia vaihtoehtoja voidaan valita. Kysymykset 10,13,15 ovat avoimia, se tarkoittaa, että vastaaja vastaa kysymykseen vapaassa muodossa itsenäisesti. Kysymykset 7,9,11,14,16,18 ovat avustavia. Niiden tarkoituksena on selventää, konkretisoida tai täydentää pääkysymyksiä. Jotta määrittellään vastaajien mielipiteet tai asenteet käytetään Likert-asteikkoa.

Loppukysymykset 19, 20 ovat suljettuja, niiden avulla arvioidaan vastaajan ominaispiirteitä. Niiden kysymysten sijainnin tavoitteena on säilyttää vastaajan suotuisa psykologinen asenne ja poistaa vaara, että kysely ei tule koskaan valmiiksi.

6.3 Tutkimustulokset

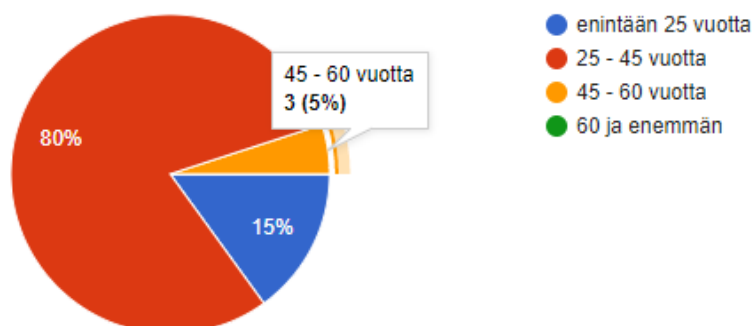
Tässä luvussa käsitellään kerättyjä tietoja aiheesta "Kryptovaluuttojen louhinnan ekosysteemi" tehdystä kyselytutkimuksesta. Kysymyksiin vastasi yhteensä 60 vastaajaa. Tutkimustulokset esitetään tekstin ja kuvioiden muodossa.

6.3.1 Vastaajien sukupuoli

Ensimmäisessä kysymyksessä kysyttiin vastaajien sukupuolta. Yhteensä saatiin 60 vastausta, 100% vastaajista on miehiä.

6.3.2 Vastaajien ikä

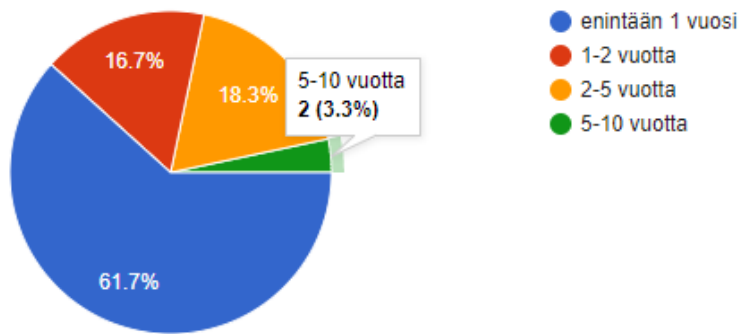
Toisessa kysymyksessä kartoitettiin vastaajien ikää. Vastaajat jaettiin neljään ikäryhmään: enintään 25 vuotta/alle 25-vuotiaat, 25–45 vuotta/ 25–45 - vuotiaat, 45–60 vuotta/ 45–60 - vuotiaat, 60 ja enemmän/ 60- ja yli 60-vuotiaat. Saatiin seuraavat tulokset: 80 % vastaajista on ikäryhmässä 25–45 vuotta, 15 % vastaajista on alle 25-vuotiaita ja vain 5 % on ikäryhmässä 45–60 vuotta. Yhteensä saatiin 60 vastausta, vastaajista yksikään ei ollut 60-vuotias tai sitä vanhempi. Tulokset on esitetty kuviossa 3.



Kuvio 3. Vastaajien ikä

6.3.3 Vastaajien kokemukset kryptovaluuttojen louhintatoiminnasta

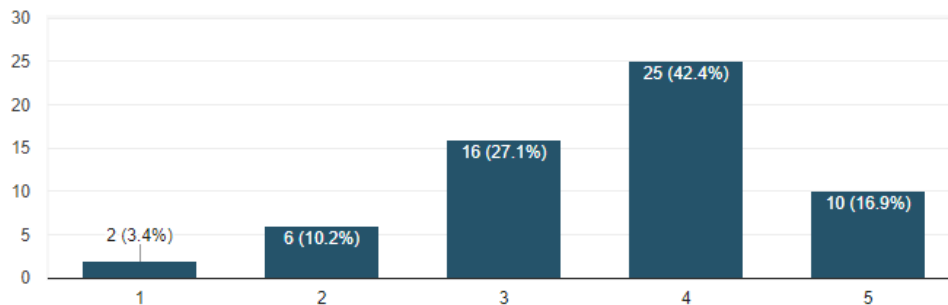
Tässä kysymyksessä tutkittiin vastaajien kokemusta, jota mitattiin ajanjaksolla, jolloin vastaajat osallistuivat kryptovaluuttojen louhintatoimintaan. Vastaajia pyydettiin arvioimaan sitä neljän aikavälin avulla: alle vuosi, 1-2 vuotta, 2-5 vuotta ja 5-10 vuotta. Saadut tulokset on esitetty kuviossa 4, ne ovat seuraavat: 61.7 % osallistuu louhintatoimintaan alle vuoden, 18.3 % - 2-5 vuotta, 16.7 % - 1-2 vuotta ja 3.3 % - 5-10 vuotta. Yhteensä saatiin vastaajilta 60 vastausta.



Kuvio 4. Vastaajien kokemukset kryptovaluuttojen louhintatoiminnasta

6.3.4 Vastaajien taitojen arviointi kryptovaluuttojen louhintatoiminnan alalla

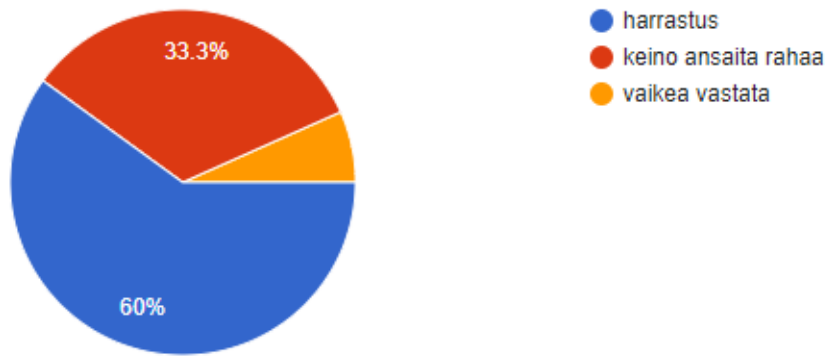
Neljännessä kysymyksessä vastaajia pyydettiin arvioimaan omia taitojaan kryptovaluuttojen louhintatoiminnan alalla asteikolla 1-5. Tähän kysymykseen saatiin 59 vastausta. Omia taitojaan arvioi viidellä pisteellä 16.9 % vastaajista, arvosanan „4“ valitsi itselleen 42.4 % vastaajista, „3“ – 27.1 % vastaajista, „2“ – 10.2 % ja 3.4 % vastaajista arvioi omia taitojaan yhdellä pisteellä. Tulokset on esitetty kuviossa 5.



Kuvio 5. Vastaajien taitojen arviointi kryptovaluuttojen louhintatoiminnan alalla

6.3.5 Henkilökohtainen suhtautuminen louhintatoimintaan

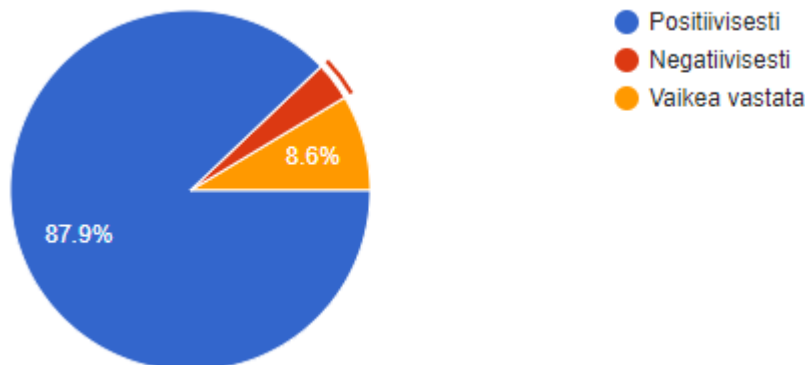
Kysymyksessä numero 5 vastaajia pyydettiin arvioimaan suhtautumista louhintatoimintaan ja valitsemaan sopiva vastaus seuraavista vaihtoehdoista: harrastus, keino ansaita rahaa ja vaikea vastata. Kuviossa 6 voi nähdä seuraavat tulokset: 60 % vastaajista katsoo, että louhintatoiminta on heidän harrastuksensa, 33.3 % vastaajista käyttää sitä keinona ansaita rahaa ja 6.7 % ei osaa vastata. Tähän kysymykseen saatiin 60 vastausta.



Kuvio 6. Henkilökohtainen suhtautuminen louhintatoimintaan

6.3.6 Kryptovaluuttojen louhintatoiminnan tulevaisuuden arviointi

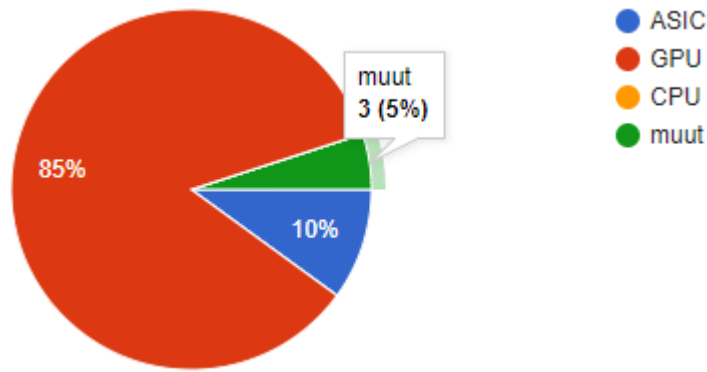
Kysymyksessä numero 19 tutkittiin vastaajien suhtautumista louhintatoiminnan tulevaisuuteen. Vastaajia pyydettiin arvioimaan louhintatoiminnan tulevaisuutta: positiivinen, negatiivinen tai määrittelemätön. Saatiin seuraavat tulokset: 87.9 % arvioi tulevaisuutta positiivisesti, 8.6 % ei osaa vastata ja vain 3.4 % katsoo tulevaisuuteen negatiivisesti. Tähän kysymykseen saatiin 58 vastausta. Tulokset on esitetty kuviossa 7.



Kuvio 7. Kryptovaluuttojen louhintatoiminnan tulevaisuuden arviointi

6.3.7 Laitteet

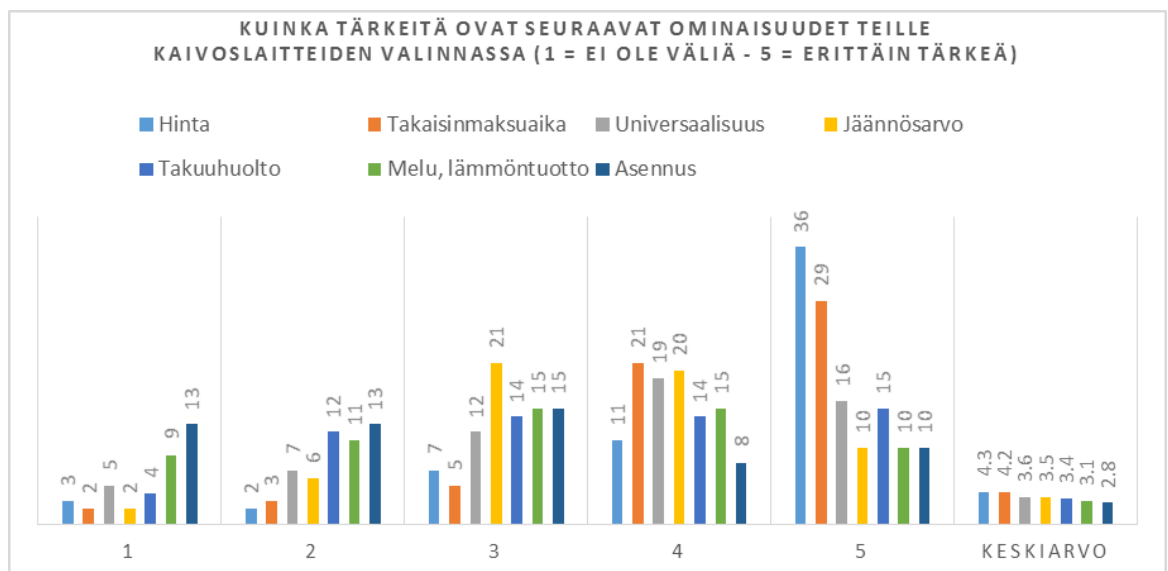
Vastaajien käyttämiä laitteita koskevaa teemaa tutkittiin kysymyksessä numero kuusi. Yhteensä saatiin 60 vastausta. Tulokset voi nähdä kuviosta 8. Pääosa vastaajista eli 85 % käyttää GPU kryptovaluuttojen louhintatoiminnassa, 10 % käyttää ASIC ja 5 % käyttää muita laitteita. Yksikään vastaajista ei käytä CPU kryptovaluuttojen louhintatoiminnassa.



Kuvio 8. Laitteet

6.3.8 Laitteiden ominaisuudet

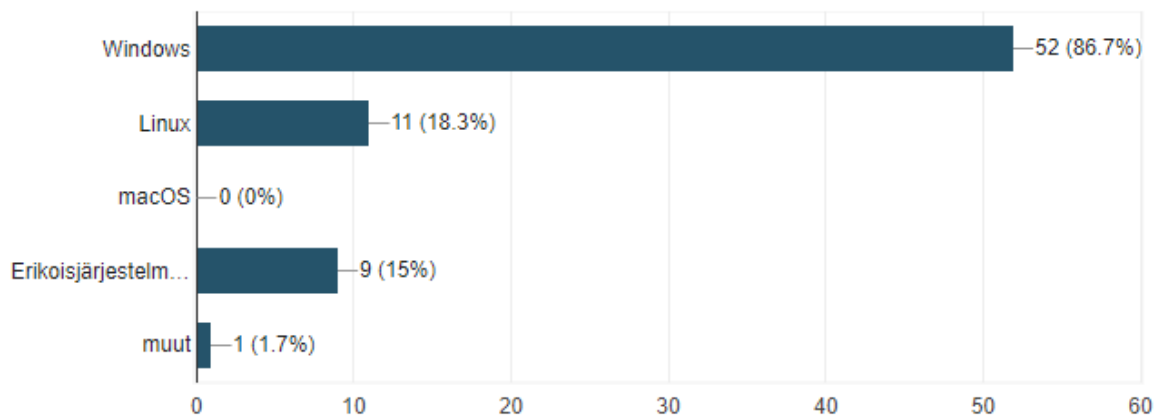
Kysymyksessä numero 7 vastaajia pyydettiin arvioimaan laitteiden ominaisuuksia asteikolla 1-5 (1 = ei ole väliä - 5 = erittäin tärkeä) seuraavan luettelon perusteella: hinta, helppo asennus, melu ja lämmöntuotto, universaalisuus, takuuhuolto, takaisinmaksuaika, jäännösarvo. Tärkeysarvioinnissa käytettiin saatujen arvioiden keskiarvoa. Saatiin seuraavat tulokset laskevassa järjestyksessä: hinta (4.3), takaisinmaksuaika (4.2), universaalisuus (3.6), jäännösarvo (3.5), takuuhuolto (3.4), melu ja lämmöntuotto (3.1), asennus (2.8). Yksityiskohtaisempia tietoja jokaista ominaisuutta koskevien arvioiden määrästä kvantitatiivisen ekvivalentin muodossa voidaan löytää kuvioista 9. Saatujen vastausten määrä jokaisen ominaisuuden osalta on vähintään 59.



Kuvio 9. Laitteiden ominaisuudet

6.3.9 Käyttöjärjestelmät

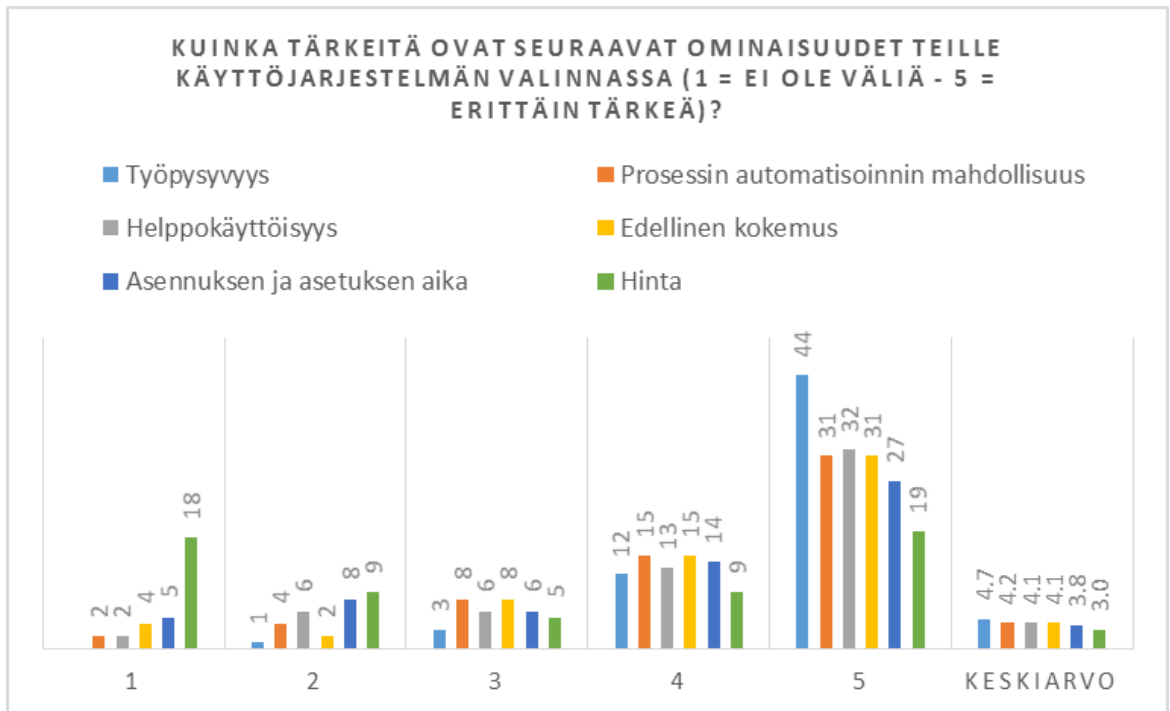
Kysymyksessä numero kahdeksan tutkittiin, mitä käyttöjärjestelmiä käyttävät vastaajat kryptovaluuttojen louhintatoiminnassa. Vastaajille tarjottiin seuraavat vastausvaihtoehdot: Windows, Linux, macOS, Erikoisjärjestelmät (SimpleMining OS, ethOS jne.) ja muut. Yhteensä saatiin 60 vastausta. Vastaajalla oli mahdollisuus valita yksi tai useampi vaihtoehto. Vastaukset järjestettiin seuraavaan prosenttien mukaiseen järjestykseen: 86,7 % vastaajista käyttää käyttöjärjestelmää Windows, 18,3 % - Linux, 15 % käyttää erikoisjärjestelmiä ja 1,7 % muita käyttöjärjestelmiä. Yksikään vastaajista ei käytä macOS. Tulokset on esitetty kuviossa 10.



Kuvio 10. Käyttöjärjestelmät

6.3.10 Käyttöjärjestelmien ominaisuudet

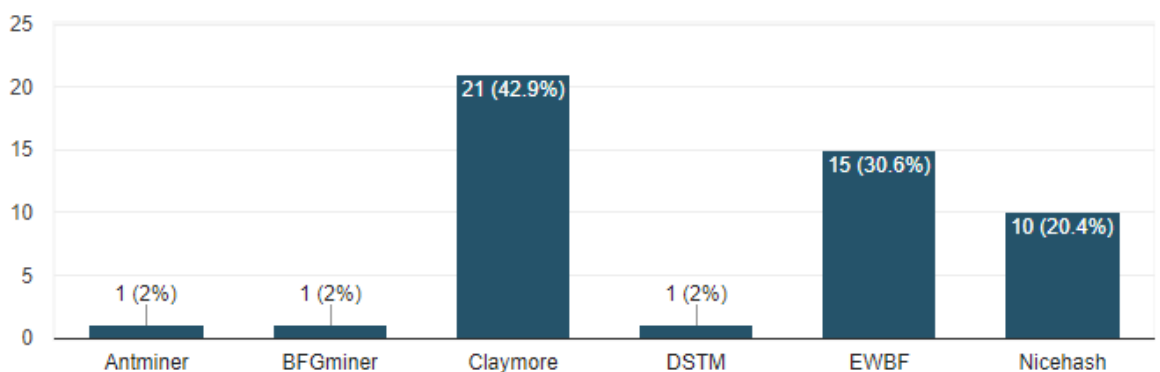
Tässä kysymyksessä (numero 9) vastaajia pyydettiin arvioimaan asteikolla 1-5 (1 = ei ole väliä - 5 = erittäin tärkeä) käyttöjärjestelmien seuraavia ominaisuuksia: edellinen kokemus, helppokäyttöisyys, asennuksen ja asetuksen aika, työpysyvyys, prosessin automatisoinnin mahdollisuus, hinta. Kyselyn tuloksena saatiin vähintään 59 vastausta, joiden keskiarvot järjestettiin laskevaan järjestykseen: työpysyvyys (4.7), prosessin automatisoinnin mahdollisuus (4.2), helppokäyttöisyys (4.1), edellinen kokemus (4.1), asennuksen ja asetuksen aika (3.8), hinta (3.0). Tarkemmat tiedot niistä ovat kuviossa 11.



Kuvio 11. Käyttöjärjestelmien ominaisuudet

6.3.11 Client-ohjelmisto

Kysymyksessä numero 10 vastaajia pyydettiin vastaamaan itse kysymykseen mitä client-ohjelmistoa ne käyttävät. Saatiin 49 vastausta ja kuusi erilaista vastausvaihtoehtoa. Prosentuaalisessa suhteessa järjestettiin vastaukset seuraavaan laskevaan järjestykseen: Claymore (42.9 %), EWBF (30.6 %), Nicehash (20.4 %), DSTM (2 %), BFGminer (2 %), Antminer (2 %). Tulokset on esitetty kuviossa 12.

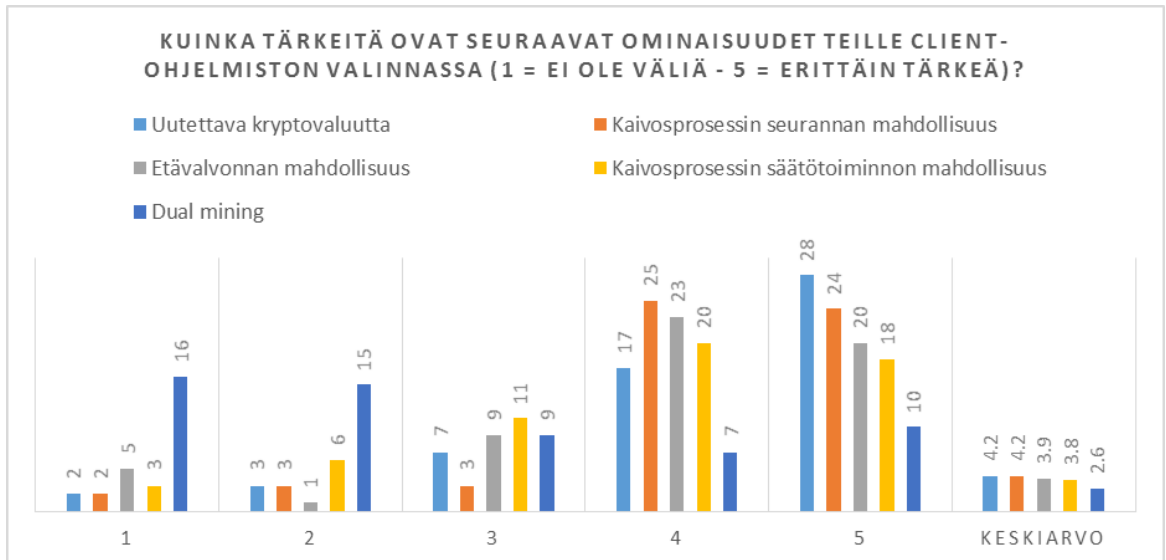


Kuvio 12. Client-ohjelmisto

6.3.12 Client-ohjelmiston ominaisuudet

Kysymyksessä numero 11 tutkittiin vastaajille tärkeimpiä client-ohjelmiston ominaisuuksia. Vastaajia pyydettiin arvioimaan asteikolla 1-5 seuraavia ominaisuuksia: kaivosprosessin

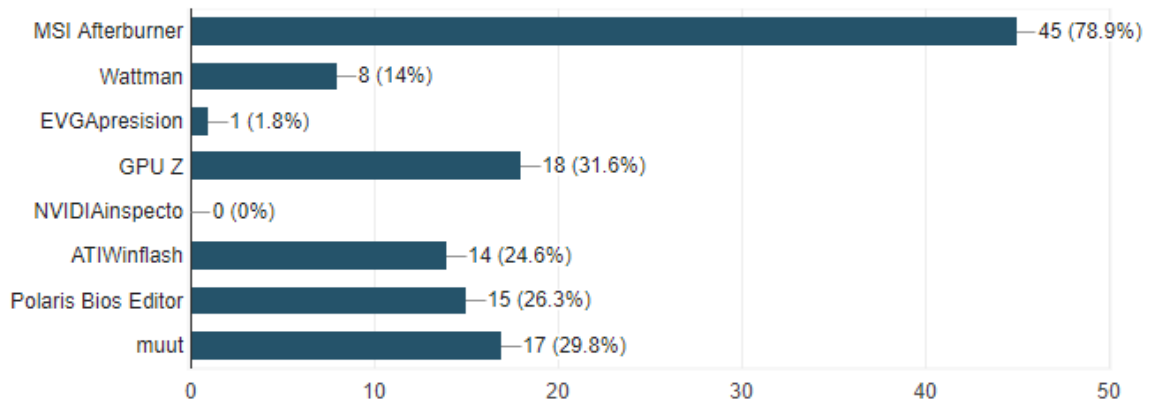
säätötoiminnon mahdollisuus, kaivosprosessin seurannan mahdollisuus, etävalvonnan mahdollisuus, uutettava kryptovaluutta, dual mining. Edellä lueteltujen ominaisuuksien tärkeysarvioinnissa käytettiin saatujen arvioiden keskiarvoa. Yhteensä saatiin vähintään 57 vastausta ja seuraavat tulokset: uutettava kryptovaluutta (4.2), kaivosprosessin seurannan mahdollisuus (4.2), etävalvonnan mahdollisuus (3.9), kaivosprosessin säätötoiminnon mahdollisuus (3.8), dual mining (2.6). Tarkemmat tiedot niistä ovat kuviossa 13.



Kuvio 13. Client-ohjelmiston ominaisuudet

6.3.13 Optimointiohjelmistot

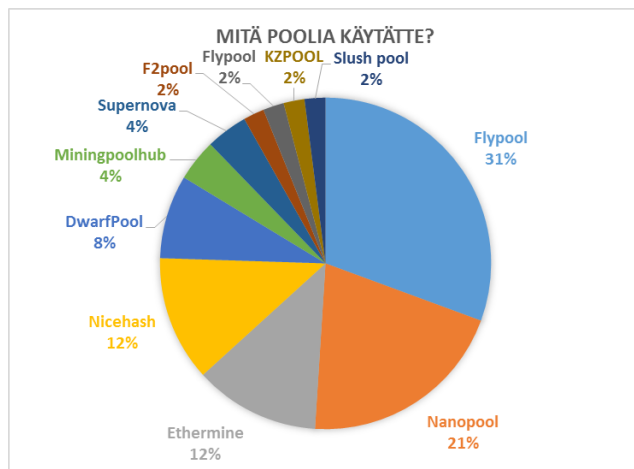
Kysymyksessä numero 12 tutkittiin mitä lisäohjelmistoa käytetään louhintalaitteiden konfigurointiin ja optimointiin. Vastaajille tarjottiin seuraavat vastausvaihtoehdot ja mahdollisuus valita yksi tai useampi vaihtoehto: MSI Afterburner, Wattman, EVGApresision, GPU Z, NVIDIAinspecto, ATIWinflash, Polaris Bios Editor, muut. Saatiin 57 vastausta ja seuraavat tulokset: 78.9 % tähän kysymykseen vastanneista käyttää MSI Afterburner, 31.6 % GPU Z, 29.8 % muut, 26.3% Polaris Bios Editor, 24.6 % ATIwinflash, 14 % Wattman, 1.8 % EVGApresision.



Kuvio 14. Optimointiohjelmit

6.3.14 Kaivosaltaat

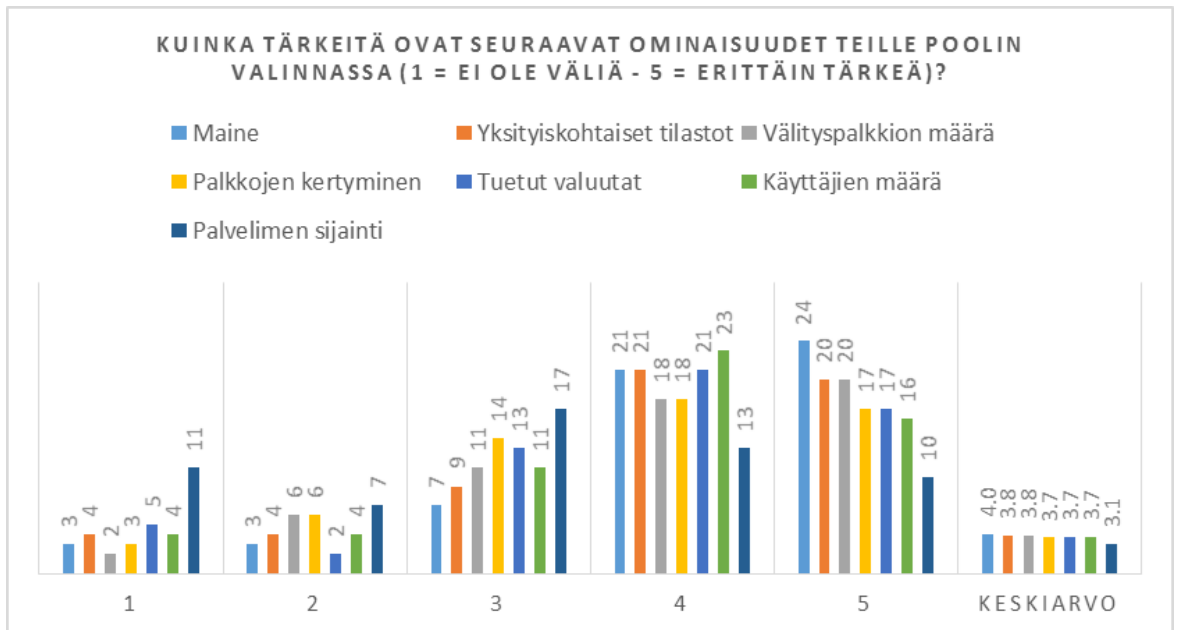
Käytettäviä kaivosaltaita koskevaan avoimeen kysymykseen numero 13 saatiin 49 vastausta ja yksitoista erilaista vastausvaihtoehtoa. Kuviossa 15 voidaan nähdä prosentuaalisessa suhteessa seuraavat tulokset: 31 % Flypool, 21 % Nanopool, 12 % Ethermine, 12 % Nicehash, 8 % DwarfPool, 4 % Miningpoolhub, 4 % Supernova, 2 % F2pool, 2 % Flypool, 2 % KZPOOL, 2 % Slush pool.



Kuvio 15. Kaivosaltaat

6.3.15 Kaivosaltaiden ominaisuudet

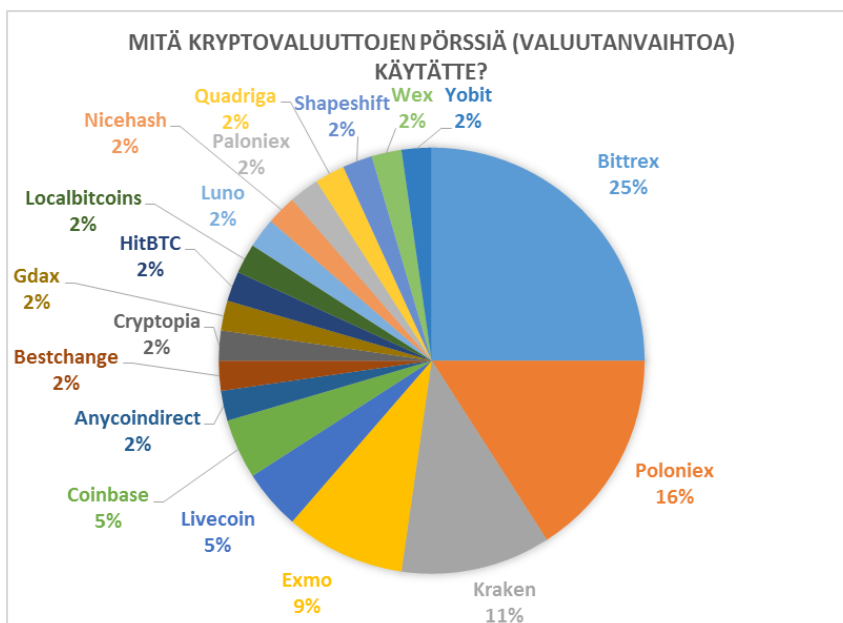
Tässä kysymyksessä (14) vastaajat arvioivat kryptovaluuttojen kaivosaltaiden ominaisuuksia asteikolla 1-5 (1 = ei ole väliä - 5 = erittäin tärkeä). Tarjottiin seitsemän ominaisuutta: maine, käyttäjien määrä, välityspalkkion määrä, palkkojen kertyminen, palvelimen sijainti (Eurooppa, Venäjä jne.), tuetut valuutat, yksityiskohtaiset tilastot. Saatiin vähintään 57 vastausta, laskettiin vastaajien arvioiden keskiarvo ja saatiin seuraavat tulokset: maine (4.0), yksityiskohtaiset tilastot (3.8), välityspalkkion määrä (3.8), palkkojen kertyminen (3.7), tuetut valuutat (3.7), käyttäjien määrä (3.7), palvelimen sijainti (3.1). Tarkemmat tiedot niistä ovat kuviossa 16.



Kuvio 16. Kaivosaltaiden ominaisuudet

6.3.16 Kryptovaluuttojen pörssi

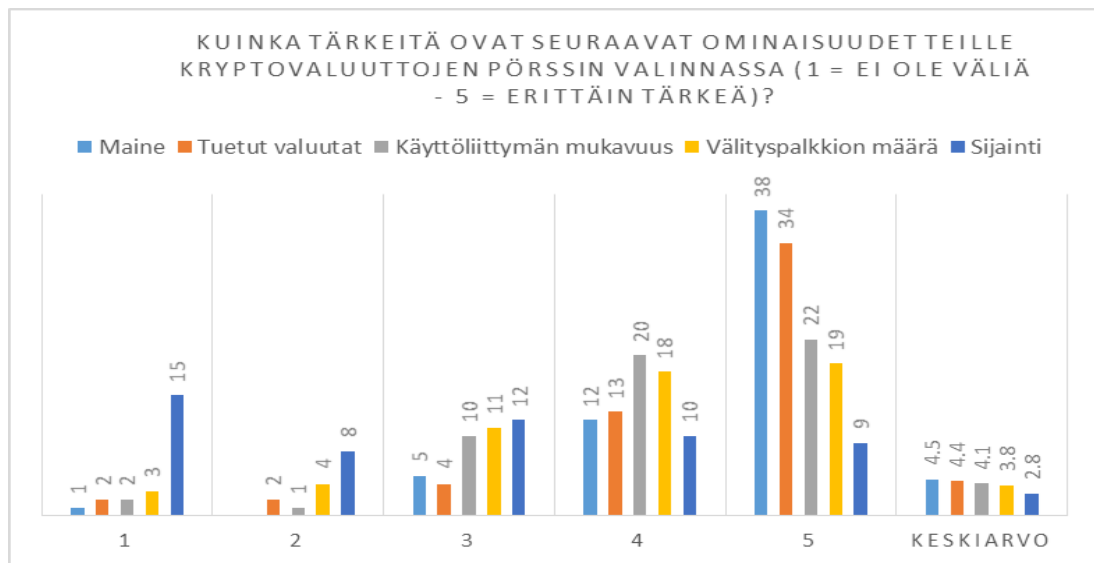
Avoimeen kysymykseen numero 15, joka näyttää mitä kryptovaluuttojen pörssiä vastaajat käyttävät, saatiin 44 vastausta, jotka koskevat 19 erilaista pörssiä. Vastausten jakautuminen prosentuaalisessa suhteessa on esitetty hyvin selvästi kuviossa 17. Tässä on mahdollista erottaa kuusi vastausta, joiden kokonaisosuus vastausten kokonaismäärästä on 71 %: Bittrex (25 %), Poloniex (16 %), Kraken (11 %), Exmo (9 %), Livecoin (5 %) ja Coinbase (5 %).



Kuvio 17. Kryptovaluuttojen pörssi

6.3.17 Kryptovaluuttojen pörssien ominaisuudet

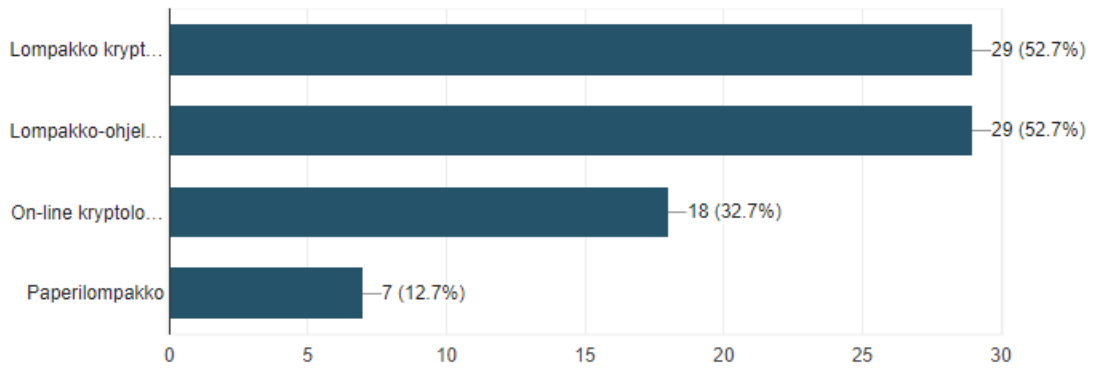
Kryptovaluuttojen pörssien ominaisuuksien arviointia varten vastaajien oli vastattava kysymykseen numero 16. Kysymyksessä arvioitiin 5 eri ominaisuutta asteikolla 1-5 (1 = ei ole väliä - 5 = erittäin tärkeä): maine, välityspalkkion määrä, sijainti (Eurooppa, Venäjä jne.), tuetut valuutat, käyttöliittymän mukavuus. Saatiin vähintään 54 vastausta seuraavalla keskimääräisellä tuloksella: maine (4.5), tuetut valuutat (4.4), käyttöliittymän mukavuus (4.1), välityspalkkion määrä (3.8), sijainti (2.8).



Kuvio 18. Kryptovaluuttojen pörssien ominaisuudet

6.3.18 Kryptolompakot

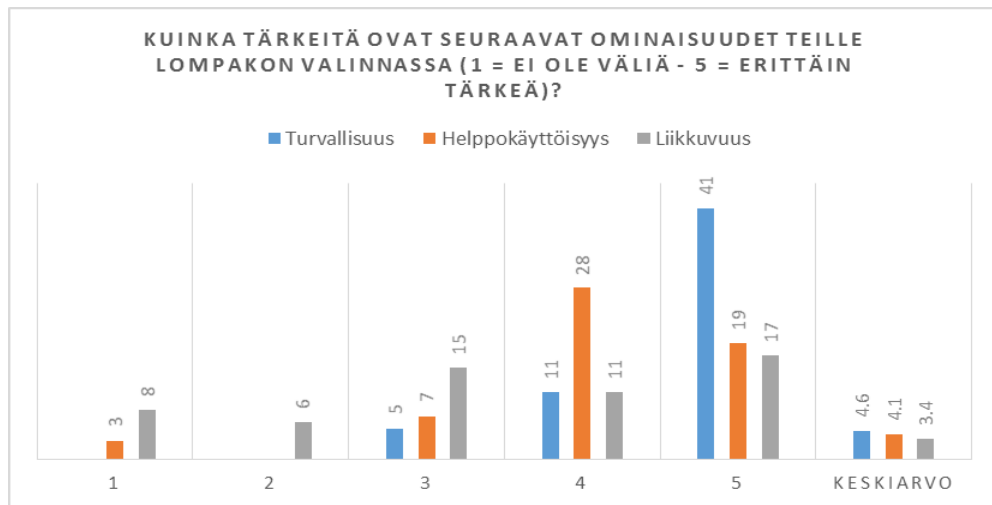
Kysymyksessä numero 17 tutkittiin vastaajien käyttämien kryptolompakoiden eri tyyppejä. Vastaajille tarjottiin neljä olemassa olevaa kryptolompakoiden tyyppiä: lompakko kryptovaluuttojen pörssillä, lompakko-ohjelma, on-line kryptolompakko, paperilompakko. Vastaajilla oli mahdollisuus valita yksi tai useampi vastausvaihtoehto. Prosentuaalisessa suhteessa jokaista vaihtoehtoa varten saatiin seuraavat tulokset: lompakko kryptovaluuttojen pörssillä (52.7 %), lompakko-ohjelma (52.7 %), on-line kryptolompakko (32.7 %), paperilompakko (12.7 %).



Kuvio 19. Kryptolompakot

6.3.19 Kryptolompakoiden ominaisuudet

Kysymyksessä numero 18 vastaajien oli arvioitava asteikolla 1-5 seuraavia ominaisuuksia: turvallisuus, helppokäyttöisyys, liikkuvuus (on olemassa Internet-yhteys). Jokaista ominaisuutta varten saatiin vähintään 57 vastausta. Kryptolompakoiden ominaisuuksien arvioiden keskiarvot järjestettiin seuraavaan laskevaan järjestykseen: turvallisuus (4.6), helppokäyttöisyys (4.1), liikkuvuus (3.4).



Kuvio 20. Kryptolompakoiden ominaisuudet

7 Pohdinta

7.1 Tulosten luotettavuus

Tässä opinnäytetyössä tehty tutkimus on kvantitatiivinen. Tämän menetelmän valinta perustuu selkeään käsitykseen siitä, mikä on tutkittava ja missä määrin saadut tulokset täyttävät tutkimus- ja käytännön tehtäville asetetut tavoitteet. Voi arvioida, että tehty tutkimus on luotettava, objektiivinen ja pätevä.

Tutkimuksen luotettavuus perustuu siihen, että tutkittava ryhmä on homogeeninen. Tämä tarkoittaa, että ryhmän jäsenillä on keskenään samanlaisia ominaisuuksia: sukupuoli, ikä, ammatillinen valmistelu, psykologinen tila. Tutkimuksen luotettavuuteen vaikutti positiivisesti myös tutkittavan alan vakaus. Suoritettavan tutkimuksen tyyppi ja sen muoto mahdollistaa säilyttämään tutkimuksen yhdenmukaisuuden tiukan säätelyn avulla.

Tutkimusta voidaan myös pitää päteväenä, koska systemaattisen tai satunnaisen virheen todennäköisyys on äärimmäisen pieni. Tutkimuksen rakenne ja tutkimukseen liittyvät kysymykset ovat huolellisesti harkittuja ja heijastavat kaikkia tutkimuksen tärkeitä näkökohtia. Esimerkiksi kun arvioidaan tai valitaan kryptovaluuttojen louhinnan ekosysteemin elementti, tutkitaan ihanteellisen objektin ominaispiirteitä, mikä mahdollistaa vertailemaan saatuja tuloksia ja arvioimaan niiden luotettavuutta.

Suoritettavan tutkimuksen objektiivisuus varmistetaan sillä, että menetelmiin ja tuloksiin eivät vaikuta henkilökohtaiset intressit, puolueellisuus, taloudelliset edut ja muut subjektiiviset tekijät. Kyselyyn perustuvan tutkimuksen suorittaminen, suuri määrä vastauksia, niiden objektiivinen käsittely ja tulkinta sekä tutkiminen teoreettisessa osassa ja ilmiön havainnointi mahdollistavat objektiivisten tietojen hankkimisen.

7.2 Johtopäätökset

Tämän tutkimuksen tärkein tehtävä oli selvittää kryptovaluuttojen louhinnan optimaaliset työkalut, mukaan lukien laitteet, käyttöjärjestelmä, client-ohjelmisto, kaivosallas, pörssi, lompakko, säätö- ja optimointiohjelmisto.

Tätä aihetta tutkittiin kysymyksissä 6-17. Saadut vastaukset heijastavat louhijoiden mielipiteitä, joiden perusteella tehtiin johtopäätökset. Tulokset ovat luonteeltaan suositeltavia, koska kryptovaluuttaan liittyviä riskejä ei otettu huomioon tässä tutkimuksessa.

Tutkimustulosten mukaan hinta ja takaisinmaksuaika ovat tärkeimmät kriteerit louhintalaitteita valittaessa. Tämän perusteella 85 % vastaajista käyttää mieluummin grafiikkaprosessoreita ja pitää niitä tärkeimpänä keinona kryptovaluuttojen tuotannossa.

Teoreettisen osan perusteella voidaan olettaa, että käyttöjärjestelmänä käytetään yleisimmin Linuxia, jolla on enemmän vakautta ja luotettavuutta. Mutta tutkimustulosten mukaan noin 87 % vastaajista käyttää Windows-käyttöjärjestelmää ja pitää sitä luotettavana. Sellainen tulos voi johtua käyttäjien aikaisemmista kokemuksista, koska käyttöjärjestelmien käyttäjiin liittyvien tilastotietojen mukaan Windowsilla on eniten käyttäjiä, se kattaa 90 prosenttia markkinoista.

Client-ohjelmistoa valittaessa 42,9 % pitää parempana Claymore-ohjelmistoa, joka toimii suosituimpien algoritmien Ethash ja Equihash kanssa. Myös kannattaa kiinnittää huomiota EWBF-ohjelmistoon, koska sitä käyttää noin 30 % vain Equihash-algoritmilla työskentelevistä vastaajista.

Noin 31 % vastaajista ei kiinnitä huomiota kaivosaltaan sijaintiin ja käyttää Flypool-ohjelmistoa sen hyvän maineen takia. Kannattaa kiinnittää huomiota siihen, että Flypool kuuluu Bitfly gmbh: lle, joka omistaa kaivosaltaan Ethermine, jonka indeksi on 12 %. Näiden indikaattorien yhteenvedon perusteella voidaan tehdä johtopäätös, että 43 % vastaajista valitsee Bitfly gmbh: n kaivosaltaat, joissa altaan nimi määrittää ainoastaan tuotettavan valuutan.

Tärkeimpänä kryptovaluuttojen myynti- tai vaihtovalustana pitävät useimmat vastaajat (25 %) Bittrexia. Voidaan huomata, että kyselyyn osallistuneiden käyttäjien mielestä on olemassa 18 muuta luotettavaa kaupankäyntialustaa, jotka täyttävät omien käyttäjien tarpeet.

Kryptovaluutan säilyttämiseen käytetään yhtä paljon sekä lompakkoja kryptovaluuttojen pörssissä että ohjelmisto-lompakkoja käyttäjien tietokoneilla. Tämä voidaan selittää niin, että on kätevämpää tehdä kauppoja pörssissä olevan lompakon avulla ja kerätä varoja on parempi tietokoneella käyttäen ohjelmisto-lompakkoa. Niitä kryptolompakkoita käyttäjät pitävät luotettavina ja helppokäyttöisinä.

Laitteiden säätämiseen ja optimointiin 78,9 % kyselyyn osallistuneista käyttää MSI Afterburneria, jota voidaan pitää tärkeimpänä ohjelmana videokorttien toiminnan säätämiseen ja valvontaan. Lisäksi noin 25 % käyttäjistä muuttaa videokorttien BIOS:n standardiasetuksia käyttäen ohjelmistoja ATI Winflash ja Polaris Bios editor.

Ottaen huomioon tehty tutkimus ja tehdyt johtopäätökset, optimaaliset työkalut voidaan kuvata seuraavasti. Näytönohjaimet, jotka perustuvat tuottajien AMD ja NVIDIA uusimpiin grafiikkaprosessoreihin Windows-käyttöjärjestelmän hallinnalla, optimointiin käytetään kolmea ohjelmaa (MSI Afterburner, ATI Winflash, Polaris Bios -editori). Valuuttaa tuotetaan Bitfly gmbh:n omistamissa kaivosaltaissa Flypool ja Ethermine client-ohjelmiston Claymore avulla. Tuotettu kryptovaluutta säilytetään ohjelmisto-lompakoissa, myyntiä tai vaihtoa varten siirretään valuutta kaupankäyntialustalle Bittrex.

7.3 Jatkokehitys- ja tutkimusehdotukset

Tutkimus tehtiin kahdella kielellä osallistujamäärän lisäämiseksi, mutta tutkimuksen tuloksista kävi ilmi, että tämä ei riitä. Indikaattoria voidaan parantaa käyttämällä kyselyssä aasialaisia kieliä, koska suurin osa kryptovaluuttoista tuotetaan Kiinassa ja suurin kaupankäyntimäärä on Japanin, Kiinan ja Etelä-Korean valuuttamarkkinoilla.

Jatkotutkimuksissa objektiivisuuden lisäämiseksi voidaan yrittää sisällyttää vastaajien ryhmään yrityksiä, jotka harjoittavat ammattimaisesti kryptovaluuttojen louhintatoimintaa. Niin voidaan laajentaa tutkimusta tämän aiheen taloudellisessa osassa. Esimerkiksi energiankulutuksia, kustannuksia, laitteiden jäähdytystä ja sijoittamista koskevat kysymykset ovat erittäin tärkeitä, koska tärkeimmät kustannukset koostuvat edellä mainituista tekijöistä.

On myös hyödyllistä selvittää, mitkä komponenttien ja laitteiden valmistajat ovat suosituimpia ja mistä syistä. Koska virtalähteet, emolevyt, prosessorit ja muut niihin liittyvät laitteet voivat vaikuttaa toiminnan luotettavuuteen ja vakauteen.

Jatkotutkimuksissa olisi otettava huomioon se, että tämän työn teoreettinen osa voi tulevaisuudessa vaatia lisäyksiä ja korjauksia, koska lohkoketjun teknologia kehittyä tällä hetkellä hyvin nopeasti ja tieto menettää nopeasti aktualisuutta.

7.4 Oman oppimisen arviointi

Opinnäytetyö kuvastaa tietoja ja taitoja, jotka olen saanut opintojen aikana. Se osoittaa kykyä analysoida ja syntetisoida tutkimusaiheeseen liittyvää aineistoa, kykyä ratkaista ongelmia, kehittää omia ideoita ja esittää argumentteja.

Opinnäytetyön kirjoittaminen kesti kolme kuukautta syksyllä 2017. Suurimman osan tehdyistä työstä muodostavat teoreettisen osan kirjoittaminen ja kvantitatiivisen tutkimuskyselyn suorittaminen.

Teoreettinen osa mahdollisti kryptovaluuttojen louhinnan ekosysteemiä koskevan aiheen täyden (ei pintapuolisen) tutkimisen. Tämän kysymyksen aktualisuus antoi mahdollisuuden tutkia ja analysoida aihetta sekä vertailla näkökulmia, käyttäen nykyaikaista kirjallisuutta ja muita ajankohtaisten tietojen lähteitä.

Asetettujen kysymysten tutkiminen toteutettiin Internet-kyselyn avulla kahden viikon kuluessa. Mielestäni tällä osalla oli suurin riski ja monimutkaisuus, koska saada vastaajat kiinnostumaan ja saada vastaukset kysymyksiin ei ollut helppoa. Oli tarve löytää yhteinen kieli ja oikea motivaatio, minkä seurauksena kyselyn tavoite täyttyi.

Opinnäytetyön kirjoittaminen oli mielenkiintoista, koska se ei ollut jonkun kirjoittamien tieteellisten teosten uudelleen kirjoittaminen, vaan minun vakava tutkimustyöni, jossa pystyin muotoilemaan ja tutkimaan ongelmaa, joka kiinnostaa monia ihmisiä.

Lähteet

BitFury Group 2015. Proof of Stake versus Proof of Work (White Paper). Luettavissa: <http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf>. Luettu: 25.9.2017.

Bitcoin Wiki 2015a. ASIC. Luettavissa: <https://en.bitcoin.it/wiki/ASIC>. Luettu: 25.9.2017.

Bitcoin Wiki 2017a. Comparison of mining pools. Luettavissa: https://en.bitcoin.it/wiki/Comparison_of_mining_pools. Luettu: 27.9.2017.

Bitcoin Wiki 2017b. Wallet. Luettavissa: <https://en.bitcoin.it/wiki/Wallet>. Luettu: 1.10.2017.

Bitcointalk 2014a. Linux vs. Windows in mining? Luettavissa: <https://bitcointalk.org/index.php?topic=357346.0>. Luettu: 25.9.2017.

Bitcointalk 2017a. Claymore's Dual Ethereum AMD+NVIDIA GPU Miner v10.1 (Windows/Linux). Luettavissa: <https://bitcointalk.org/index.php?topic=1433925>. Luettu: 27.9.2017.

Bitcointalk 2017b. OFFICIAL CGMINER mining software thread for linux/win/osx/mips/arm/r-pi 4.10.0. Luettavissa: <https://bitcointalk.org/index.php?topic=28402.0>. Luettu: 26.9.2017.

Bitcoinmining 2016. Bitcoin mining pools. Luettavissa: <https://www.bitcoinmining.com/bitcoin-mining-pools/>. Luettu: 26.9.2017.

Blockgeeks 2017a. What Is Hashing? Under The Hood Of Blockchain. Luettavissa: <https://blockgeeks.com/guides/what-is-hashing/>. Luettu: 25.9.2017.

Blockgeeks 2017b. Best Cryptocurrency Exchanges: The Ultimate Guide. Luettavissa: <https://blockgeeks.com/guides/best-cryptocurrency-exchanges/>. Luettu: 27.9.2017.

Blockgeeks 2017b. Cryptocurrency Wallet Guide: A Step-By-Step Tutorial. Luettavissa: <https://blockgeeks.com/guides/cryptocurrency-wallet-guide/>. Luettu: 04.10.2017.

Coinhills.com 2017. All Digital Currency Exchanges Volume Ranking. Luettavissa: <https://www.coinhills.com/market/exchange/>. Luettu: 4.10.2017.

Coinpursuit 2017. How do digital currency exchanges work. Luettavissa: <https://www.coinpursuit.com/articles/how-do-digital-currency-exchanges-work.138/>. Luettu: 4.10.2017.

Coinmarketcap 2017a. Coinmarketcap.com. Luettavissa: <https://coinmarketcap.com/>. Luettu: 23.9.2017.

Cryptocompare.com 2017a. Compare Bitcoin, Ethereum and Litecoin Mining Equipment. Luettavissa: <https://www.cryptocompare.com/mining/#/equipment>. Luettu: 27.9.2017.

Cryptocompare.com 2017b. What is Multi-pool mining? Luettavissa: <https://www.cryptocompare.com/mining/guides/what-is-multi-pool-mining/>. Luettu: 24.9.2017.

Ethereum Community Forum 2017 .Ubuntu or Windows for mining ETH. Luettavissa: <https://forum.ethereum.org/discussion/4401/ubuntu-or-windows-for-mining-eth>. Luettu: 25.9.2017.

ethOS 2017. ethOS Mining OS. Luettavissa: <http://ethosdistro.com/>. Luettu: 26.9.2017.

Heikkilä, T. 2014. Kvantitatiivinen tutkimus. Luettavissa: <http://www.tilastollinentutkimus.fi/1.TUTKIMUSTUKI/KvantitatiivinenTutkimus.pdf>. Luettu: 17.10.2017

Investopedia 2017. Bitcoin Exchange. Luettavissa: <http://www.investopedia.com/terms/b/bitcoin-exchange.asp>. Luettu: 2.10.2017.

KvantiMOTV 2010. Kyselylomakkeen laatiminen. Luettavissa: <http://www.fsd.uta.fi/menetelmaopetus/kyselylomake/laatiminen.html>. Luettu: 20.10.2017.

Miningclub.info 2017. Windows vs Linux. . Luettavissa: <http://miningclub.info/threads/windows-vs-linux.731/>. Luettu: 25.9.2017.

Newsbtc 2016. A Brief History of Bitcoin and Bitcoin Mining. Luettavissa: <http://www.news-btc.com/2016/05/26/brief-history-bitcoin-bitcoin-mining/>. Luettu: 23.9.2017..

Nicehash 2017a. Profitability calculator. Luettavissa: <https://www.nicehash.com/profitability-calculator>. Luettu: 26.9.2017.

Netmarketshare.com 2017a. Desktop Operating System Market Share. Luettavissa: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpssp=2017&qpnp=1&qptimeframe=Y&qpcustomd=0>. Luettu: 23.9.2017.

PiMP OS 2017. Portable Instant Mining Platform. Luettavissa: <https://getpimp.org/>. Luettu: 26.9.2017.

Pool mining 2017. Hardening Stratum, the Bitcoin Pool Mining Protocol. Luettavissa: <https://arxiv.org/abs/1703.06545>. Luettu: 26.9.2017.

Simplemining 2017. SimpleMining Mining Operating System. Luettavissa: <https://simplemining.net/>. Luettu: 26.9.2017.

Steemit 2017. WINDOWS vs. LINUX - which one is better for mining crypto? Luettavissa: <https://steemit.com/cryptocurrency/@lifipp/windows-vs-linux-which-one-is-better-for-mining-crypto-face-to-face-comparison>. Luettu: 25.9.2017.

Swan, M. 2017. Blockchain: Blueprint for a New Economy. Olimp-Business. Moskva.

USC 2017. Organizing Your Social Sciences Research Paper: Quantitative Methods. Luettavissa: <http://libguides.usc.edu/writingguide/quantitative>. Luettu: 20.10.2017.

Wikipedia 2017a. Cryptocurrency. Luettavissa: <https://en.wikipedia.org/wiki/Cryptocurrency>. Luettu: 20.9.2017.

Wikipedia 2017b. Operating system. Luettavissa: https://en.wikipedia.org/wiki/Operating_system. Luettu: 23.9.2017.

Wikipedia 2017c. Linux(ydin). Luettavissa: [https://fi.wikipedia.org/wiki/Linux_\(ydin\)](https://fi.wikipedia.org/wiki/Linux_(ydin)). Luettu: 23.9.2017.

Whattomine 2017a. Whattomine.com. Luettavissa: <https://whattomine.com/coins>. Luettu: 20.9.2017.

Whattomine 2017b. Whattomine.com. Luettavissa: <https://whattomine.com/asic>. Luettu: 24.9.2017.

Liitteet

Liite 1. Kyselylomake

Kryptovaluuttojen louhinnan ekosysteemi

1. Sukupuoli

- Mies
- Nainen

2. Ikä

- enintään 25 vuotta
- 25 - 45 vuotta
- 45 - 60 vuotta
- 60 ja enemmän

3. Kuinka kauan olette osallistuneet kryptovaluuttojen kaivostoimintaan?

- enintään 1 vuosi
- 1-2 vuotta
- 2-5 vuotta
- 5-10 vuotta

4. Kuinka hyväksi arvioitte taitonne kryptovaluuttojen kaivostoiminnan alalla?

	1	2	3	4	5	
erittäin huono	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	erinomainen

5. Kaivostoiminta on Teitä varten:

- harrastus
- keino ansaita rahaa
- vaikea vastata

6. Miltä laitteita käytätte mieluummin kaivostoiminnassa?

- ASIC
- GPU
- CPU
- muut

7. Kuinka tärkeitä ovat seuraavat ominaisuudet Teille kaivoslaitteiden valinnassa (1 = ei ole väliä - 5 = erittäin tärkeä)

	1	2	3	4	5
Hinta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Helppo asennus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Melu, lämmöntuotto	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Universaalisuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Takuuhuolto	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Takaisinmaksuaika	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jäännösarvo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. Mitä käyttöjärjestelmää käytätte kaivostoiminnassa?

- Windows
- Linux
- macOS
- Erikoisjärjestelmät (SimpleMining OS, ethOS jne.)
- muut

9. Kuinka tärkeitä ovat seuraavat ominaisuudet Teille käyttöjärjestelmän valinnassa (1 = ei ole väliä - 5 = erittäin tärkeä)

	1	2	3	4	5
Edellinen kokemus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Helppokäyttöisyys	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Asennuksen ja asetuksen aika	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Työpysyvyys	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prosessin automatisoinnin mahdollisuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hinta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

10. Mitä client-ohjelmistoa käytätte?

Your answer

11. Kuinka tärkeitä ovat seuraavat ominaisuudet Teille client-ohjelmiston valinnassa (1 = ei ole väliä - 5 = erittäin tärkeä)

	1	2	3	4	5
Kaivosprosessin säätötoiminnon mahdollisuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kaivosprosessin seurannan mahdollisuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Etävalvonnan mahdollisuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uutettava kryptovaluutta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dual mining	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

12. Mitä ohjelmistoa käytätte laitteiden optimointiin ja konfigurointiin?

- MSI Afterburner
- Wattman
- EVGApresision
- GPU Z
- NVIDIAinspecto
- ATIWinflash
- Polaris Bios Editor
- muut

13. Mitä poolia käytätte?

Your answer _____

14. Kuinka tärkeitä ovat seuraavat ominaisuudet Teille poolin valinnassa (1 = ei ole väliä - 5 = erittäin tärkeä)

	1	2	3	4	5
Maine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Käyttäjien määrä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Välityspalkkion määrä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Palkkojen kertyminen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Palvelimen sijainti (Eurooppa,Venäjä jne.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tuetut valuutat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Yksityiskohtaiset tilastot	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

15. Mitä kryptovaluuttojen pörssiä (valuutanvaihtoa) käytätte?

Your answer

16. Kuinka tärkeitä ovat seuraavat ominaisuudet Teille kryptovaluuttojen pörssin valinnassa (1 = ei ole väliä - 5 = erittäin tärkeä)

	1	2	3	4	5
Maine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Välityspalkkion määrä	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sijainti (Eurooppa,Venäjä jne.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tuetut valuutat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Käyttöliittymän mukavuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17. Kryptovaluutan säilyttämiseksi käytätte:

- Lompakko kryptovaluuttojen pörssillä
- Lompakko-ohjelma
- On-line kryptolompakko
- Paperilompakko

18. Kuinka tärkeitä ovat seuraavat ominaisuudet Teille lompakon valinnassa (1 = ei ole väliä - 5 = erittäin tärkeä)

	1	2	3	4	5
Turvallisuus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Helppokäyttöisyys	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Liikkuvuus (on olemassa Internet-yhtäisyys)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

19. Kuinka arvioitte kryptovaluutan kaivostoiminnan tulevaisuutta?

- Positiivisesti
- Negatiivisesti
- Vaikea vastata

20. Aiotteko kasvattaa kaivoskapasiteettia lähitulevaisuudessa?

- Kyllä
- Ei
- Vaikea vastata