ANALYYSI

Kvanttilaskenta tulee - onko rahoitusala valmiina?

Rahoitusvakaus | 27.05.2025 | Heli Snellman, Joonas Savolainen, Antti Hirvonen

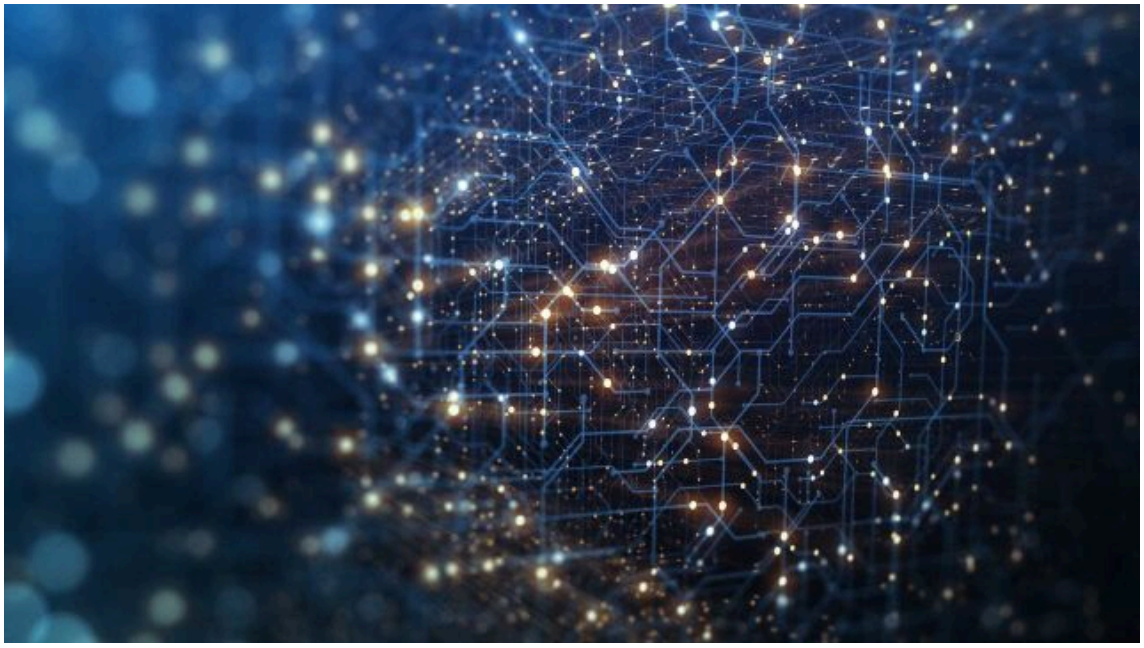
KIRJOITTAJAT

Heli Snellman
Vanhempi neuvonantaja

Joonas Savolainen
Tietoasiantuntija

Antti Hirvonen
Data-asiantuntija

Suomen Pankki toteutti alkuvuodesta 2025 kyselytutkimuksen rahoitustoimialalle kvanttiteknologian näkymistä, hyödyistä ja riskeistä. Vastausten perusteella kvanttiteknologia saattaa muuttaa liiketoimintaa merkittävästi pitkällä aikavälillä. Testauksia ja käytännön toteutuksia on tehty kuitenkin vasta vähän, koska teknologia on kypsymätöntä. Mahdollisuuksina nähdään muun muassa riskienhallinnan ja tietoturvan paraneminen sekä sijoitustoiminnan kehittyminen. Toisaalta myös riskeissä korostuu huoli tietoturvasta.



Teknologian kehittyminen ja digitalisaatio ovat muokanneet suuresti käyttämiämme pankkipalveluja viimeisen kolmenkymmenen vuoden aikana. Osa teknologisesta kehityksestä näkyy asiakkaille suoraan, osa on enemmän konepellin alla olevia taustajärjestelmiä. Yksi tällä hetkellä nopeasti kehittyvä ilmiö on kvanttiteknologia. Sillä saattaa olla suuria vaikutuksia monella yhteiskunnan sektorilla, myös rahoitustoimialalla.

Kvanttitietokoneet eroavat perinteisistä tietokoneista perustavanlaatuisella tavalla.[1] Kvanttitietokoneet hyödyntävät kvanttimekaniikan ilmiöitä, kuten superpositiota ja lomittumista, minkä ansiosta ne ovat erityisen tehokkaita tietyissä laskentatehoa vaativissa tehtävissä.[2] Kvanttilaskennan hyötyjen toteutuminen edellyttää, että kvanttitietokoneet sisältävät nykyistä suuremman määrän kvanttitietokoneen perusyksiköitä eli kubitteja. Yhtä tärkeää on, että kubittien häiriöalttiutta saadaan pienennettyä. Kolmantena edellytyksenä on kvanttilaskennan erityispiirteitä hyödyntävien algoritmien ja ohjelmistojen kehittyminen. Kaikissa näissä on tapahtunut viime vuosina merkittävää edistystä. Moniin ongelmiin klassinen tietokone on kuitenkin jatkossakin kvanttitietokonetta sopivampi työkalu, eli eri laskentatavat tulevat olemaan toisiaan täydentäviä.

Hyötyjen ohella digitalisaatio ja uudet teknologiat tuovat mukanaan uusia riskejä, eikä kvanttiteknologia tee tästä poikkeusta. Tulevaisuudessa kvanttitietokoneilla voidaan todennäköisesti muun muassa murtaa nykyisiä salausalgoritmeja.[3] Kvanttilaskennasta aiheutuviin tietoturvariskeihin varautuminen on jo ajankohtaista, vaikka nykyisillä kvanttitietokoneilla ei salausalgoritmeja pystytäkään murtamaan. Salattuja tietoja voidaan nimittäin varastaa jo nyt ja säilöä siihen asti, että kvanttiteknologia on riittävän kehittynyttä murtamaan näiden salauksen. Toinen esimerkki riskeistä on digitaalisten allekirjoitusten väärentäminen.

Kvanttilaskennasta aiheutuviin tietoturvariskeihin on kehitetty kvanttiturvallisia algoritmeja. Niiden standardoinnissa otettiin suuri askel elokuussa 2024, kun Yhdysvaltain standardisointi- ja teknologiainstituutti NIST julkaisi standardisoidut kvanttiturvalliset algoritmit. Suomessa Traficom on lisännyt NISTin standardoimat algoritmit kansalliseen kriteeristöön ja suosittelee organisaatioita siirtymään kvanttiturvallisten algoritmien käyttöön mahdollisimman pian.

Kvanttiteknologiassa nähdään paljon potentiaalisia hyötyjä

Suomen Pankki toteutti helmikuussa 2025 kyselyn rahoitustoimialalle kvanttiteknologian näkymistä, hyödyistä ja riskeistä. Vapaaehtoiseen kyselytutkimukseen vastasi yhteensä noin 30 Suomessa toimivaa rahoitusalan yritystä. Vastaajajoukkoon sisältyy mm. pankkeja, vakuutusyhtiöitä, rahastoyhtiöitä ja sijoituspalveluyrityksiä.

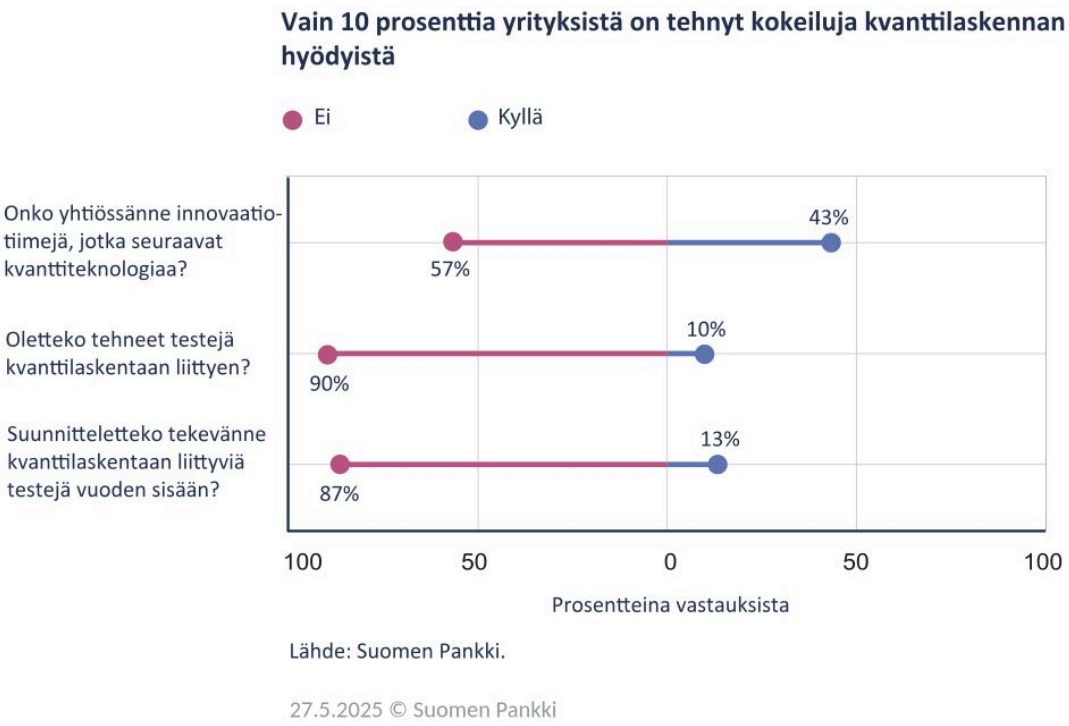
Vastaajia pyydettiin arvioimaan kvanttiteknologian mahdollisuuksia omin sanoin. Yleisesti nähtiin, että yhtäältä nykyistä laskentaa ja mallinnusta voidaan tehdä nopeammin, tehokkaammin ja tarkemmin ja toisaalta kvanttilaskenta mahdollistaa täysin uudenlaisten ongelmien ratkaisun. Suurimpina kvanttilaskennan mahdollisuuksina vastaajat pitivät riskienhallinnan ja tietoturvan paranemista sekä sijoitustoiminnan kehittymistä. Toisaalta viidesosa vastaajista ei nähnyt hyötyjä kvanttiteknologiasta omalle liiketoiminnalleen ainakaan tällä hetkellä.

Lähes puolet vastaajista arvioi kvanttiteknologian tuovan hyötyjä riskienhallintaan. Esimerkkeinä mainittiin rahanpesun estäminen, petosten torjunta ja yleisesti erilaisten riskien mallintaminen. Lisäksi kvanttiteknologian nähtiin mahdollistavan nykyistä monipuolisempien ja monimutkaisempien riskisimulaatioiden, stressitestausten ja skenaarioanalyysien tekemisen. Sijoitustoiminnan osalta hyötyjä odotetaan sijoitussalkun optimointiin, johdannaisten hinnoitteluun ja markkina-analyysiin. Nämä potentiaaliset kvanttiteknologian käyttökohteet ovat hyvin linjassa Kansainvälisen järjestelypankin (BIS) tutkimuksen kanssa, jossa on listattu mahdollisia kvanttiteknologian hyötyjä rahoitussektorilla.[4]

Käytännön toteutuksia on vasta vähän

Lähes puolella kyselyyn vastanneista rahoitusalan toimijoista on innovaatiotiimejä, jotka seuraavat kvanttiteknologian kehitystä (kuvio 1). Innovaatiotiimeissä tähän seurantaan käytetään aikaa keskimäärin alle yksi henkilötyövuosi. Lisäksi kvanttilaskennan kehitystä seurattaneen osana muuta työtä, vaikka erityistä innovaatiotiimiä ei olisikaan yrityksessä perustettu. Joka kymmenes vastaajaorganisaatio oli tehnyt testejä tai kokeiluja kvanttilaskennan hyödyntämiseksi, ja reilu kymmenen prosenttia on tekemässä testejä ja kokeiluja lähimmän vuoden aikana.

Kuvio 1.

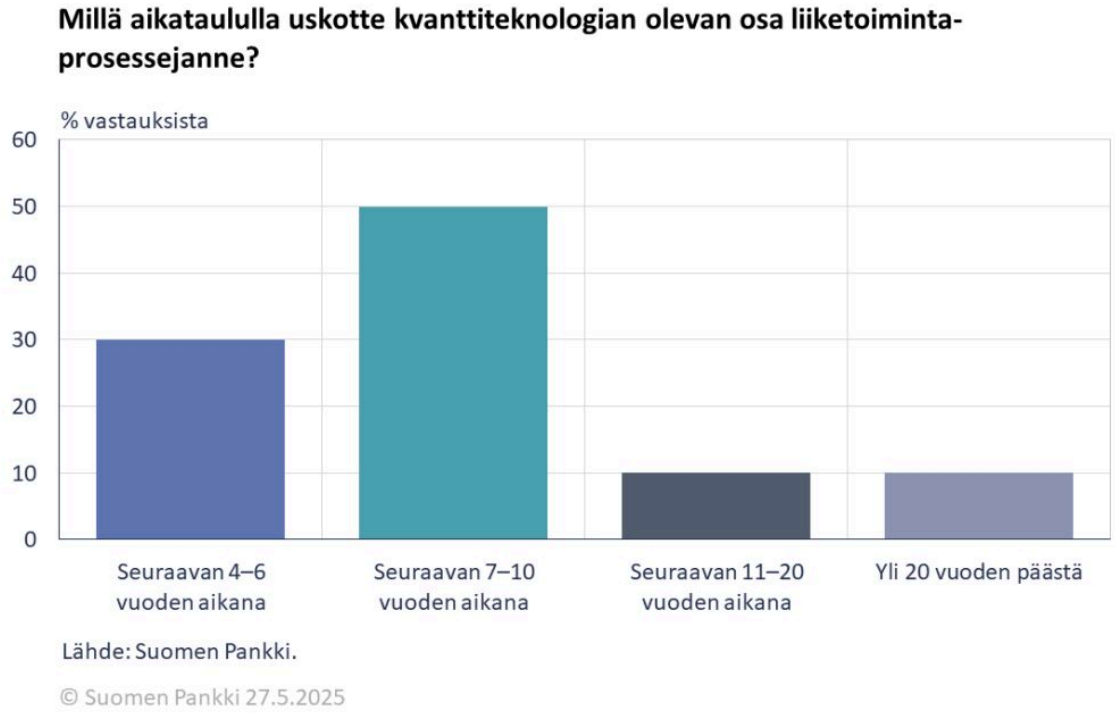


Kvanttiteknologia voi muuttaa liiketoimintaa merkittävästi pitkällä aikavälillä

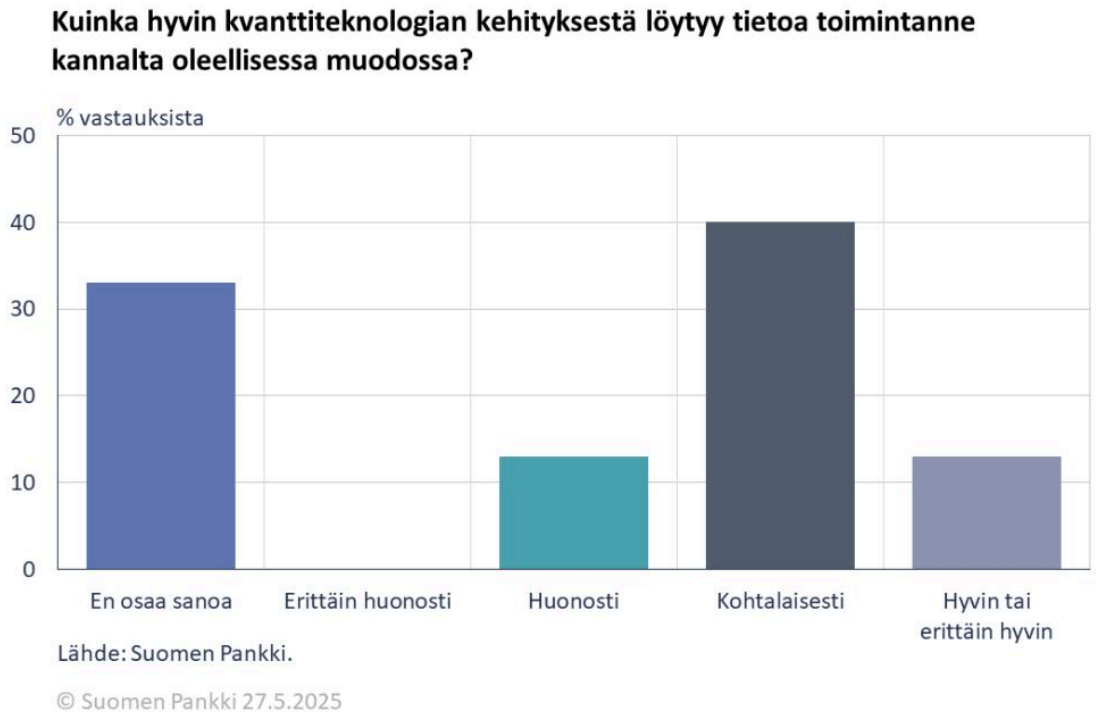
Tärkeänä tai jokseenkin tärkeänä tulevaisuuden kilpailutekijänä kvanttiteknologiaa piti kaksi kolmesta vastaajasta. Mikäli uuteen teknologiaan ei pystytä panostamaan riittävästi, vaarana on kilpailijoista jälkeen jääminen ja kilpailuaseman menettäminen. Vajaa 40 % vastaajista arvioi tällä hetkellä oman valmiutensa olevan keskimääräistä tasoa tai parempi suhteessa kotimaisiin kilpailijoihin. Valmius suhteessa ulkomaisiin kilpailijoihin nähtiin hieman heikompana, mutta toisaalta reilu puolet vastaajista ei osannut arvioida omaa valmiuttaan suhteessa kilpailijoihinsa.

Neljä viidestä kyselytutkimukseen vastanneesta rahoitustoimialan yrityksestä oli sitä mieltä, että kvanttiteknologia tulee olemaan osa liiketoimintaprosesseja seuraavan kymmenen vuoden kuluessa (kuvio 2). 40 % vastaajista koki, että tietoa kvanttiteknologiasta on oman toiminnan kannalta kohtalaisesti saatavilla ja vain reilun kymmenen prosentin mielestä tietoa oli saatavilla hyvin tai erittäin hyvin (kuvio 3).

Kuvio 2.

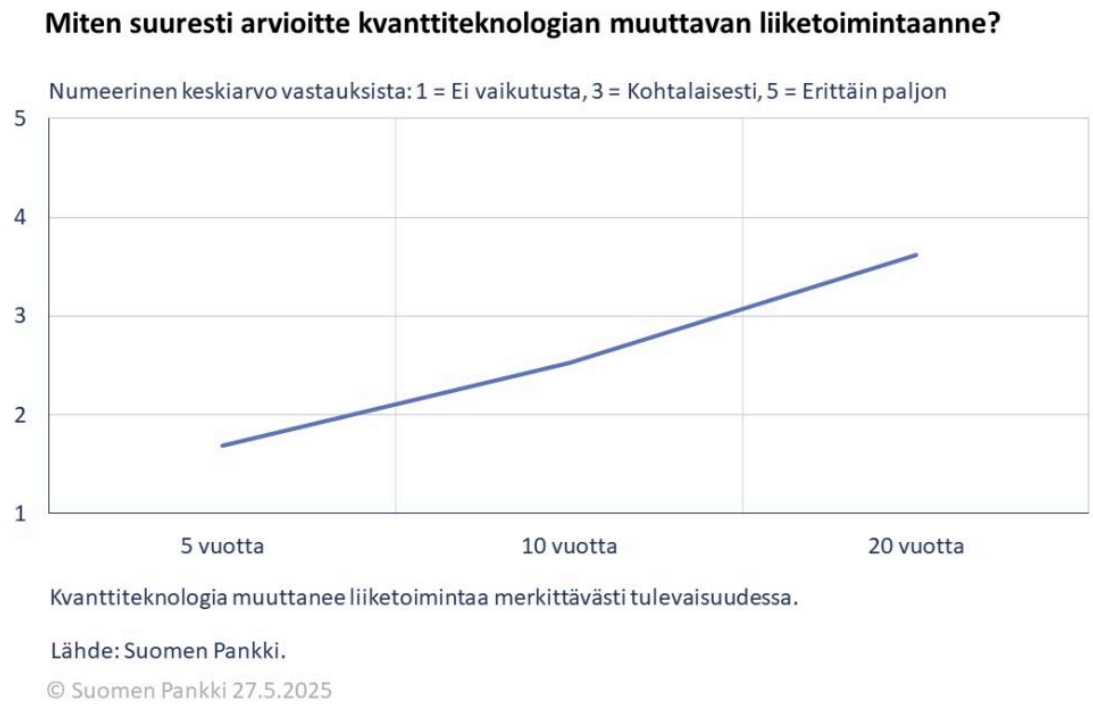

Millä aikataululla uskotte kvanttiteknologian olevan osa liiketoiminta-prosessejanne?
% vastauksista
60
50
40
30
20
10
0
Seuraavan 4–6 vuoden aikana
Seuraavan 7–10 vuoden aikana
Seuraavan 11–20 vuoden aikana
Yli 20 vuoden päästä
Lähde: Suomen Pankki.
© Suomen Pankki 27.5.2025

Kuvio 3.



Kvanttilaskennan nähtiin muuttavan pitkällä aikavälillä liiketoimintaa paljon. Seuraavan viiden vuoden aikana muutoksen ei odoteta olevan vielä kovin suuri, mutta kahdenkymmenen vuoden kuluessa vaikutukset ovat huomattavia (kuvio 4).

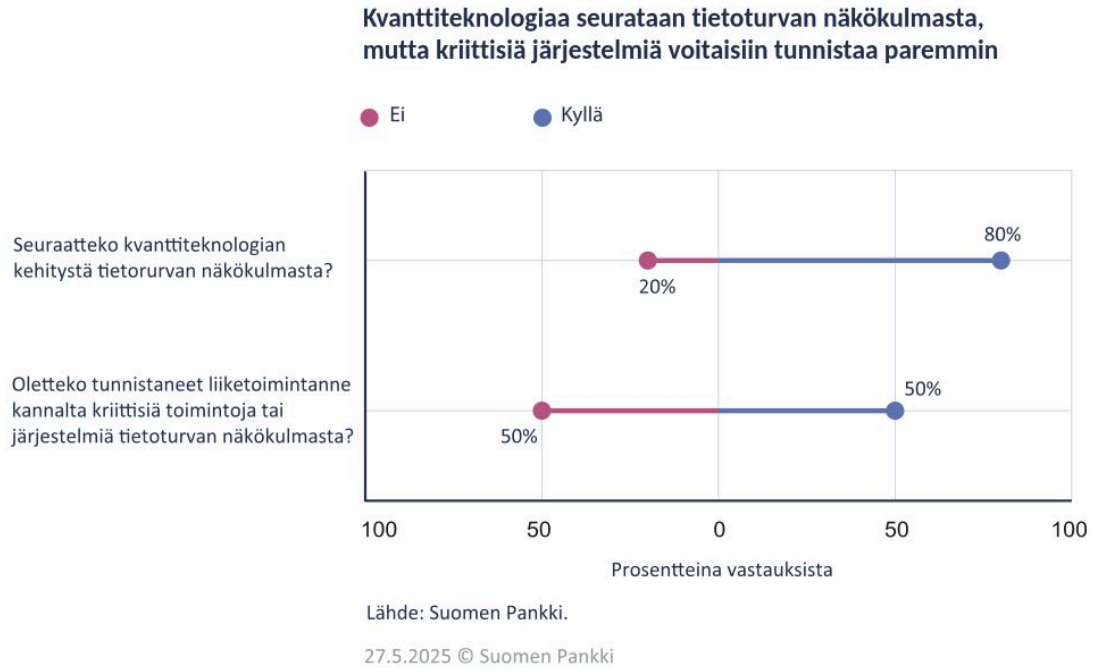
Kuvio 4.



Riskeistä korostuvat tietoturva ja erityisesti salauksen murtaminen

Suurimpina kvanttilaskennan riskeinä tunnistettiin tietoturvaan liittyvät kysymykset ja erityisesti nykyisten tietojen salauksen murtaminen. Vastanneista yrityksistä 80 % kertoi seuraavansa kvanttiteknologian kehitystä tietoturvan näkökulmasta (kuvio 5). Puolet vastanneista toimijoista on tunnistanut omassa toiminnassaan kriittisiä toimintoja tai järjestelmiä, joihin kvanttiteknologian kehityksellä voi olla vaikutusta nimenomaan tietoturvan näkökulmasta.

Kuvio 5.



Kolmasosa vastanneista oli sitä mieltä, että kvanttiteknologian mukanaan tuomiin mahdollisiin tietoturvauhkiin täytyy reagoida jo nyt. Usein suositellaan, että toimijat aloittavat kvanttiturvallisiin ratkaisuihin siirtymisen kartoittamalla käytössään olevat salausratkaisut, eli tekevät kryptoinventaarion.[5] Vastaajajoukosta vajaa puolet oli suunnitellut tekevänsä kryptoinventaarion, muttei ollut vielä toteuttanut sitä.

Neljä viidestä vastaajasta näki, että tietojen varastaminen nyt ja salauksen murtaminen tulevaisuudessa on olennainen riski. Reilu puolet vastaajista oli sitä mieltä, että kriittisimpien tietojen pitäisi pysyä salaisina vähintään 20 vuotta. Kuudesosa näki, että kriittisimpien tietojen olisi pysyttävä salattuina vähintään 10 vuotta ja 10 % näki viisi vuotta riittäväksi ajaksi. Kolmannes vastaajista sanoi, että kvanttiturvalliseen salaukseen siirtymiseen menee omalla organisaatiolla enintään kolme vuotta (kuvio 6). Yksi työkalu kvanttiuhan arviointiin on Moscan lause[6], joka kertoo, milloin kvanttiturvallisten algoritmien vaihto täytyy aloittaa. Mikäli algoritmien vaihtoon tarvittava aika ja tietojen salassapitoaika ylittävät relevantin kvanttitietokoneen kehittämiseen tarvittavan ajan, ovat tiedot mahdollisesti alttiita murrettavaksi ennen salassapitoajan päättymistä.

Kuvio 6.

Haasteina teknologian kypsymättömyys, osaamisen puute ja kustannukset

Suurimpina haasteina seuraavan viiden vuoden aikana vastaajat pitivät kvanttiteknologian kypsymättömyyttä, osaamisen puutetta ja hyödyllisten käyttötapausten puutetta (kuvio 7). Suuret kustannukset nähtiin myös ongelmaksi. Kvanttiteknologian vaikutusten arviointi pitkällä aikavälillä (seuraavan 20 vuoden aikana) koettiin erittäin haastavaksi, ja lähes puolet vastaajista koki pitkän aikavälin haasteiden arvioinnin mahdottomaksi. Vastanneet puolestaan pitivät myös pitkällä aikavälillä suuria kustannuksia ongelmana, vaikka osaamisen oletettiinkin paranevan, teknologian kypsyvän ja käyttötapauksia löytyvän.

Kuvio 7.

Erikseen kysyttiin, tuleeko nykyisestä lainsäädännöstä rajoitteita kvanttiteknologian hyödyntämiselle. 80 % vastaajista näki, että lainsäädäntö ei rajoita kvanttiteknologian hyödyntämistä. Sen sijaan viidennes vastaajista totesi rajoitteita tulevan esimerkiksi EU:n tekoälylainsäädännön, tietosuoja-asetuksen tai muun pankkien toimintaan vaikuttavan sääntelyn kautta.

Kvanttiteknologian tuloon varauduttava

Kyselytutkimuksen perusteella Suomessa toimivat rahoitustoimialan yritykset seuraavat kvanttiteknologian kehittymistä. Potentiaalisia hyötyjä on tunnistettu, mutta toisaalta kypsymätön teknologia ei ole vielä mahdollistanut kovinkaan paljon testausta. Pitkällä aikavälillä kvanttiteknologia saattaa muuttaa paljonkin rahoitusalan liiketoimintaa. Uuden teknologian mukanaan tuomia riskejä on myös arvioitu, ja huoli nykyisten tietojen salauksen murtamisesta nousee esiin vastauksissa.

Kvanttilaskenta saattaa kehittyessään mullistaa nykyiset tietotekniset ratkaisut. Siksi kaikkien rahoitusalan toimijoiden kannattaa seurata kehitystä ja miettiä, mitä kvanttilaskenta voisi tarkoittaa omalle liiketoiminnalle ja miten kvanttilaskennan tuloon täytyy varautua. Jokaisella toimijalla täytyy olla valmius toimia ja siirtyä kvanttiturvalliseen salaukseen. Rahoitusvakauden

kannalta luottamus on äärimmäisen keskeistä. Uusien uhkien toteutuminen olisi omiaan horjuttamaan asiakkaiden luottamusta digitaalisiin palveluihin. Olemassa olevien järjestelmien päivittäminen vie aikaa, ja toisaalta täytyy olla valmius päivittää myös kvanttiturvallista salausta sitä mukaa, kun kehitys etenee.

Suomessa kvanttilaskentaan on perehdytty esimerkiksi FutureQ-tutkimushankkeessa, jossa ollut edustajia useilta eri toimialoilta ja myös Suomen Pankista. Yhteistyötä eri toimijoiden kesken on tärkeää tehdä myös jatkossa niin kotimaassa[7] kuin kansainvälisestikin.

Suomen ja Euroopan on tärkeää pystyä hyödyntämään kvanttilaskennan ja muiden uusien teknologioiden tarjoamat hyödyt. Suomen kvanttiteknologiastrategia 2025-2035 julkaistiin huhtikuussa 2025.[8] Euroopan komissio on puolestaan kertonut työohjelmassaan julkaisevansa EU:n kvanttistrategian vuoden 2025 toisen vuosineljänneksen aikana.

Yhteisenä tavoitteenamme tulee olla se, että Suomi ja Eurooppa ovat pysyvästi kvanttilaskennan kärkijoukkoa. Kvanttilaskenta täytyy osaltaan valjastaa tukemaan kilpailukykyämme ja iskunkestävyyttämme.

Viitteet

1. Ks. VTT:n julkaisu ”Kvanttilaskenta: Käytännön matkaopas tulevaisuuteen”, luvut 2-3. ↑
2. Kvanttilaskenta uusien innovaatioiden lähteenä finanssimarkkinoilla – Euro ja talous ↑
3. Esimerkiksi Shorin algoritmilla, ks. VTT:n julkaisu ”Kvanttilaskenta: Käytännön matkaopas tulevaisuuteen”, luku 7. ↑
4. Quantum computing and the financial system: opportunities and risks. Myös World Economic Forumin ja Accenturen raportissa arvioidaan ja kuvataan rahoitusalan käyttötapauksia: Quantum technology | World Economic Forum (sivut 29-31 ja 49-50). ↑
5. Ks. esimerkiksi Huoltovarmuuskeskuksen julkaisu, s. 15-18. ↑
6. Ks. Huoltovarmuuskeskuksen julkaisu, s. 4. ↑
7. Suomalainen esimerkki yhteistyöstä on The Finnish Quantum Institute, https://instituteq.fi/ ↑
8. Suomen kvanttiteknologiastrategia 2025–2035 : Suomen uusi kasvun moottori ja kestävän tulevaisuuden rakentaja - Työ- ja elinkeinoministeriö ↑

Asiasanat

kvanttilaskenta, kvanttiteknologia, tietoturva