BLOGI

Kvanttilaskenta rahoitusalalla – Uhka vai mahdollisuus?

28.5.2025 – Rahoitusvakaus

KIRJOITTAJA
Matti Hellqvist
Vanhempi ekonomisti

Kvanttitietokone ja kvanttilaskenta ovat mielenkiintoisia ja mahdollisesti mullistavia uusia teknologioita. Pitkään ne vaikuttivat lähinnä teoreettiselta ja futuristiselta idealta, mutta viime vuosina kehitys on ollut nopeaa sekä tehokkaampien kvanttitietokoneiden rakentamisessa että kvantti-ilmiöitä älykkäästi hyödyntävien algoritmien saralla. Siksi on mahdollista, että kvanttilaskennasta voidaan nähdä ensimmäisiä mielekkäitä käytännön sovelluksia seuraavan kymmenen vuoden kuluessa, ellei jopa jo aivan lähivuosien aikana.

Pankit ja rahoitusjärjestelmä ovat edenneet pitkälle digitalisaatiossa. Niiden järjestelmät nojaavat laajaan datan hyödyntämiseen ja tehokkaaseen tietoliikenteeseen sekä tietoturvaan. Laadukas ydintoimintoja kuvaava data voisi antaa monia mahdollisuuksia kvanttilaskennan hyödyntämiselle. Suomalaiset rahoitusalan toimijat tunnistavat näiden mahdollisuuksien olemassaolon, mutta niiden käytännön toimet tai kokeilut kvanttitekniikkaan liittyen painottuvat vahvasti riskien hallinnan näkökulmaan. Tämä kävi ilmi Suomen pankin rahoitusalalle hiljattain tekemässä kyselyssä, jossa selvitettiin odotuksia kvanttilaskennan vaikutuksista. Onko riskeihin keskittyminen painopisteenä oikea valinta?

Shorin uhka

Yksi tunnetuimpia kvanttitietokoneen sovelluskohteita on Shorin algoritmi.[1] Tämän menetelmän avulla pystytään tehokkaasti jakamaan suuria kokonaislukuja osatekijöihinsä. Käytännössä sillä voi siis murtaa internetin turvallisen käytön yhtenä kulmakivenä nykyisin toimivan julkisen ja yksityisen avaimen salausmekanismin. Vaikka nykyisissä kvanttitietokoneissa ei vielä ole tähän riittävästi vääntöä, jo nyt on mahdollista, että salattua tietoliikennettä nauhoitetaan ja tallennetaan odottamaan salauksen murtumista tulevaisuudessa.

Salausmekanismien murtumisen riskiin varautuminen on monella tapaa jo käynnissä. Paremmin kvanttikestäviä salausmenetelmiä ollaan standardoimassa ja Euroopassa uusi

1. Ks. Shor 1994.

sääntely edellyttää finanssialalta muun muassa käytettyjen salausmenetelmien systemaattista hallinnointia. [2] Tämä edistää niin kutsuttua kryptografista ketteryyttä eli kykyä vaihtaa ja päivittää salausmenetelmiä tarvittaessa turvallisempiin. Myös keskuspankit ovat selvittäneet, kuinka kvanttimekaniikan ilmiöitä voidaan hyödyntää eri tavoin entistä vahvemman salauksen ja turvallisempien järjestelmien rakentamisessa.[3]

Shorin algoritmin muodostamalla uhka on todellinen, mutta sen toteutumiseen on vielä matkaa. Kyseinen algoritmi on yksi vaativimmista kvanttilaskennan käyttötavoista. Tämä johtuu siitä, että nykyisten kvanttitietokoneiden laskentayksiköissä eli kubiteissa on kohinaa tai häiriöitä. Niitä on oltava käytössä moninkertainen määrä, jotta kokoon saadaan edes yksi ns. looginen eli virheetön kubitti. [4] Shorin algoritmi tarvitsee toimiakseen suuren määrän loogisia kubitteja kun taas monissa muissa kvanttilaskennan sovelluksissa ensimmäisiä hyödyllisiä tuloksia voidaan saada jo pienemmillä kubittien määrällä. [5] Shorin algoritmin käytön mahdollistuminen merkittävässä mittakaavassa on siis nykytiedoilla yksi niistä kvanttilaskennan sovelluksista, jonka toteutuminen on kauimpana tulevaisuudessa.[6]

Monien mahdollisuuksien horisontti

Kvanttilaskennan positiivisia mahdollisuuksia voidaan todennäköisesti hyödyntää jo ennen sitä hetkeä, jolloin nykyiset salausmenetelmät lopulta murtuvat. Rahoitusalalla nämä uudet mahdollisuudet voivat tarkoittaa esimerkiksi kykyä ratkoa optimointitehtäviä, jotka olivat aiemmin aikarajoitteiden tai kustannuksien vuoksi käytännössä mahdottomia. Kyse voi olla vaikkapa sijoitusportfolion tarkemmasta optimoinnista tai maksujärjestelmän selvitysprosessin parannuksesta, joka vähentää prosessiin tarvitun rahan määrää. Toinen tärkeä sovelluskohde on rahoitusinstrumenttien riskien ja oikean hinnoittelun arvioiminen entistä tarkemmin tai nopeammin. Esimerkiksi johdannaisten hinnoittelussa usein käytettävää Monte Carlo -simulointien menetelmää voidaan jatkossa tehostaa kvanttilaskennalla. Tässä menetelmässä muodostetaan satunnaisesti suuri määrä havaintoja, joista kyseisen johdannaisen hinta voidaan ratkaista. Tarkempaan lopputulokseen pääseminen edellyttää Monte Carlo simuloinneissa rajusti suurempaa laskentatyötä, mutta kvanttilaskennan avulla tämä työmäärän kasvunopeus puolittuu.

Rahoitusalalle tehdyn kyselyn perusteella kvanttilaskennan soveltamisen kokeilut ovat meillä vielä olleet harvinaisia, mutta lähes puolet kyselyyn vastanneista toimijoista ainakin seuraa aktiivisesti alan kehitystä.

---

2. Ks. Yhdysvaltain standardisointi- ja teknologiainstituutti (NIST, PQC Project) sekä tammikuussa 2025 voimaan astunut voimaan astunut EU:n asetus digitaalisesta häiriönsietokyvystä (DORA).
3. Ks. Bucciol & Tiberi 2023.
4. Ensimmäistä kertaa loogisen kubitin muodostamisessa onnistuttiin vuonna 2024 useamman eri tahon toimesta. Ks esim. Quantum Insider 13.12.2024 ja Google 2024.
5. Gidney & Ekerå 2021 arvioivat tarvitsevansa Shorin algoritmilla noin 6000 loogista kubittia tai 20 miljoonaa kohinaista kubittia 2048 bittisen RSA salausavaimen murtamiseen 8 tunnin ajassa. Johdannaisten hinnoittelussa arvioitu loogisten kubittien minimimäärä on neljästä viiteen tuhatta. (Stamatopoulos & al 2024). Optimointitehtävien osalta arviot riippuvat tehtävästä, mutta ovat näitä matalampia.
6. Havainnollinen visualisointi kvanttitietokoneiden kyvyistä ja eri tehtävien vaatimuksista on esitetty Samuel Jaquesin vuosittain päivittämässä infograafissa (Jaques 2024).

Kvanttilaskennan näkymiä on luodattu laajemmin esimerkiksi VTT:n vetämässä FutureQ-projektissa, jonka tuloksia on esitetty helposti lähestyttävässä muodossa ”Kvanttilaskenta: Käytännön matkaopas tulevaisuuteen”-julkaisussa. On selvää, että uusista kyvyistä syntyy aikanaan kilpailuetua, joka voi muuttaa myös rahoitustoimialan rakenteita tai luoda uusia toimintamalleja. Äärimmillään voi jopa syntyä tilanteita, joissa tietyllä markkinalla ”voittaja vie kaiken”.

Onko kvanttilaskenta siis uhka vai mahdollisuus rahoitusalalla? Selvästikin se tuo mukanaan molempia. On tärkeää, että molemmat ulottuvuudet tunnistetaan, jotta uhkiin voidaan varautua ja mahdollisuuksiin tarttua. Pelkästään uhkiin keskittymällä vaarana on nimittäin se, että mahdollisuudet menevät ohi ja ainoastaan uhkat toteutuvat.

Lähteet

Bucciol E, Tiberi P. Quantum safe payment systems, Banca di Italia 2023

Gidney, C., and M. Ekerå. 2021. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”. https://arxiv.org/pdf/1905.09749

Google, 2024. https://blog.google/technology/research/google-willow-quantum-chip/

Jaques, Samuel. Landscape of quantum computing in 2024. Quantum Landscape 2024

NIST, PQC Project: Post-Quantum Cryptography | CSRC

DORA Regulation (Digital operational resilience act) - Full text

Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. pp. 124–134.

Stamatopoulos, N., Zeng, W. 2024. Derivative Pricing using Quantum Signal Processing – Quantum

Avainsanat

kvanttilaskenta, kvanttiteknologia, rahoitusala, Shorin algoritmi, kvanttitietokone