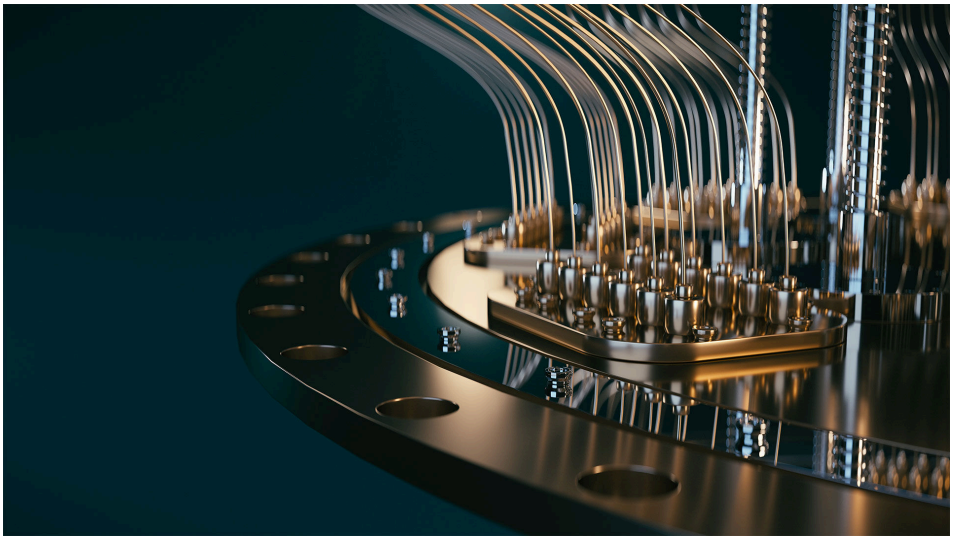
ANALYYSI

Kvanttilaskenta uusien innovaatioiden lähteenä finanssimarkkinoilla

10.1.2024 – Analyysi – Rahoitusvakaus

Lauri Jantunen
Tietostrategiapäällikkö

Useat tutkimukset lupaavat kvanttilaskennan tuovan nykyistä kehittyneempiä tapoja analysoida dataa ja suorittaa vaativaa laskentaa nopeasti ja tarkasti, mutta teknologia on vielä varsin uutta ja sen täytyy ratkaista monta perustavanlaatuista käytännön ongelmaa ennen kuin lupaukset realisoituvat. Potentiaalisten hyötyjen lisäksi kvanttilaskenta nostaa esiin myös tietoturvauhkia, jotka edellyttävät siirtymistä nykyisistä salausmenetelmistä kvanttiturvallisiin salausalgoritmeihin.



Tässä artikkelissa esitetyt mielipiteet ovat kirjoittajan omia eivätkä välttämättä edusta Suomen Pankin näkemystä.

Kvanttilaskenta mullistaa tietojenkäsittelyn

Kvanttilaskenta on perustavanlaatuisesti erilainen lähestymistapa tietojenkäsittelyyn. Kvanttitietokoneissa laskenta perustuu kubitteihin, eli kvanttibitteihin. Ne eroavat perinteisestä tietoteknologian bittikäsitteestä varsin merkittävästi. Kun klassisella bitillä voi olla vain kaksi toisensa poissulkevaa tilaa (1 ja 0), kubitit pystyvät nk. superposition avulla käsittelemään myös tiloja, jotka ovat samaan aikaan 0 ja 1. Kvanttitietokoneissa eri kubittien tila saadaan korreloitumaan toisten kubittien kanssa nk. lomittumisen kautta. Näitä kvanttimekaniikan ilmiöitä hyödyntämällä kvanttilaskennassa voidaan tehdä yhden syötteen perusteella monta eri laskutoimitusta eli päivittää monen eri kubitin tilaa samanaikaisesti, kun taas perinteiset tietokoneet voivat käsitellä yhdessä laskentaprosessissa vain yhden laskusuorituksen kerrallaan. Parhaimmillaan kvanttilaskenta voi siten tarjota huomattavia tehokkuushyötyjä[1]. Ratkaisevaa on se, sopiiko tietty ongelma kvanttitietokoneelle eli tunnetaanko sen ratkaisemiseen tehokas kvanttilaskentaa hyödyntävä tapa. Kvanttitekniikan mahdolliset hyödyt voivat siten vaihdella käyttötapausten välillä suuresti.

Tekniset ongelmat ja korkea hinta kvanttiteknologian pullonkaulana

Kvanttiteknologia on vielä alkutekijöissä ja monet tämän korkean teknologian käyttötapaukset vaativat, että nykyisten kvanttitietokoneiden ongelmat ratkaistaan ennen kuin pääsemme kunnolla hyödyntämään kvanttilaskentaa. Kubittien toteuttamista kehitetään moneen eri tekniikkaan perustuen, eikä vielä ole selvillä mikä ratkaisuista tuottaa parhaan tuloksen. Yhteinen haaste kaikissa toteutuksissa on kvanttimekaanisten ilmiöiden suuri herkkyys ulkoisille häiriöille. Pienet häiriöt voivat johtaa kvanttitilan superposition tai kubittien lomittumisen purkautumiseen[2]. Kubitteja tarvitaan kvanttitietokoneisiin mahdollisimman paljon, mutta häiriöiden riski kasvaa, kun niiden määrää lisätään. Tehokkaan kvanttitietokoneen toteuttaminen on siten hyvin vaikeaa. Viimeaikainen kehitys on ollut lupaavaa erityisesti siksi, että kubittien virheherkkyyttä tai kvanttitietokoneiden virheenkorjaamisen tasoa on saatu parannettua. Käytännössä toimivan kvanttitietokoneeseen tarvitaan riittävän vakaasti toimivien kubittien ohella keinot niiden tilan alustamiseen, ohjaamiseen ja mittaamiseen[3]. Kaiken tämän tulisi onnistua järjestelmässä, jossa kubittien määrää voidaan skaalata suuremmaksi, jotta kvanttitietokoneen laskentatehoa voidaan kasvattaa. (WEF, 2022). Näiden ongelmien ratkaiseminen mahdollistaisi vakaamman kvanttiteknologian, sekä luotettavampien ja tehokkaampien kvanttitietokoneiden rakentamisen.

Aikaisemmin yksi suurimmista esteistä kvanttilaskennan soveltamiselle on ollut myös kvanttitietokoneiden vaikea saatavuus ja näiden järjestelmien vaatimien investointien korkea hinta. Nykyään monet johtavista pilvipalveluntarjoajista, kuten Amazon ja Microsoft, ovat kuitenkin laajentaneet palvelutoimintaansa myös kvanttilaskennan tarjoamisen puolelle. Näin ollen erillisiä kalliita kvanttitietokoneita tai

---

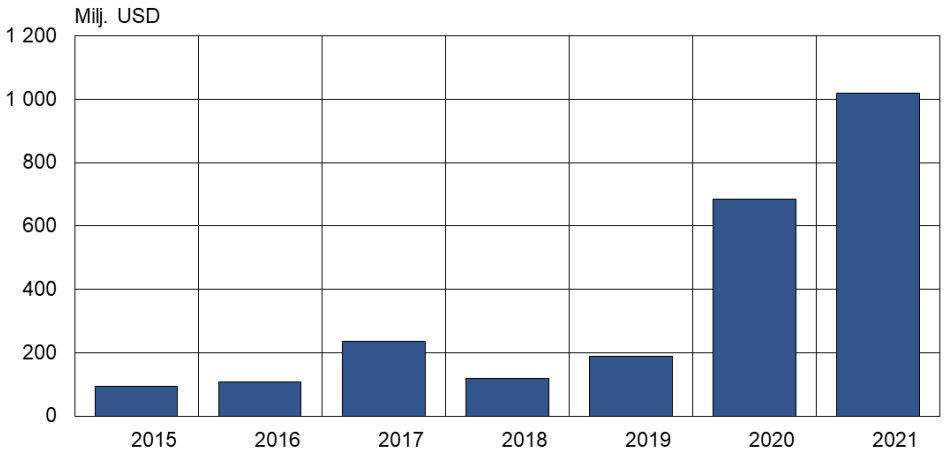
1. n-määrällä kubitteja kvanttitietokone voi laskea jopa 2^n laskua kerralla.
2. Tätä ilmiötä kutsutaan dekoherenssiksi.
3. Kvanttitietokoneen tulisi esimerkiksi täyttää DiVincenzon kriteerit.

infrastruktuuriratkaisuja ei tarvitse enää itse rakentaa, vaan kvanttikyvykkyyksiä[4] voidaan kehittää ja hankkia ketterästi ohjelmistopalveluina jotka laskutetaan käytön mukaan (nk. *software-as-a-service*).

Kvanttiteknologia kehittyy nopeaa tahtia ja moni uskoo, että monet teknologian nykyisistä ongelmista pystyttäisiin ratkaisemaan lähitulevaisuudessa, mikä näkyy myös investoinneissa. Viime vuonna kvanttiteknologiaan sijoitettiin ennätykselliset 2 miljardia euroa ja julkisen sektorin panostus teknologiaan on myös voimakkaassa kasvussa (Bogobowicz et al., 2023). Kirjoitushetkellä maailman tehokkaimmat kvanttitietokoneet ovat +1000 kubitin Atom Computing Atomic Array ja IBM Condor, joissa on yli kaksi kertaa enemmän kubitteja kuin viime vuoden lopulla julkaistussa IBM Osprey koneessa. IBM uskoo kvanttitietokoneiden kehityksen jatkuvan nopeasti.

Kuvio 1.

Riskirahoittajat ovat viime vuosina sijoittaneet voimakkaasti kvanttiteknologiaan



Lähde: Pitchbook.
© Suomen Pankki / 11.12.2023

Finanssisektori yksi kvanttilaskennan suurimmista hyötyjistä

Kvanttiteknologialla on potentiaalisesti kauaskantoisia ja laajamittaisia vaikutuksia useilla toimialoilla ja rahoitusmarkkinoita veikataan yhdeksi ensimmäisistä hyötyjistä (Ménard et al., 2020). Kvanttitietokoneilla on nähty mahdolliseksi ratkaista monia perustavanlaatuisia ongelmia rahoituksessa analysoimalla suuria määriä dataa nopeammin ja tarkemmin, kuin mitä perinteisillä tietokoneilla on mahdollista (Bouland et al., 2020). Kvanttilaskentaa onkin jo sovellettu useissa rahoitusalalle tärkeissä käyttötapauksissa, kuten johdannaisten hinnoittelussa, riskien mallinnuksessa,

4. Vaikka nämä kvanttitietokoneet ovat tällä hetkellä teholtaan enemmänkin todellisen kvanttitietokoneen prototyyppejä tai joissain tapauksissa perinteisellä laskennalla simuloituja kvanttitietokoneita, niin niiden käyttäminen vastaa kuitenkin täysin tapaa, jolla myös suuremman laskentatehon omaavaa kvanttitietokonetta voitaisiin myöhemmin käyttää. Siksi ne mahdollistavat jo nyt kvanttilaskennan hyödyntämiseen valmistautumisen ja sen edellytysten selvittämisen.

portfolion optimoinnissa ja luonnollisen kielen käsittelyssä[5] (nk. *natural language processing*) (Herman et al., 2022). Kvanttilaskennalla tulee olemaan merkittäviä vaikutuksia rahoitusalalla myös tietoturvaan liittyvissä kysymyksissä (Bailey et al., 2020).

Taulukko 1.

Kvanttilaskenta lupaa edistysaskelia useisiin eri käyttötapauksiin rahoitusalalla

Tehtäväluokka	Käyttötapaukset	Klassiset ratkaisut	Kvanttiratkaisut
Stokastinen mallinnus	Johdannaisten hinnoittelu, riskianalyysi	Koneoppiminen, Monte Carlo -menetelmät, PDE-mallit	Kvanttiteknologialla tehostettu koneoppiminen, Monte Carlo -menetelmät ja PDE-mallit
Optimointi	Ennustemallien selittäjien valinta, portfolion optimointi, kombinatoriset optimointitehtävät	Heuristiikat, BB ja IPM	Kvanttiteknologialla tehostettu optimointi
Koneoppiminen	Luonnollisen kielen mallintaminen, poikkeavuuksien tunnistaminen, riskiklusterointi	Klusterianalyysi syväoppiminen,	Kvanttiteknologialla tehostettu klusterianalyysi ja koneoppiminen

Lähde: Herman et al., 2022

Keskiössä johdannaisten hinnoittelu, optimointi ja koneoppimiskysymykset

Monissa rahoitusalan tehtävissä, kuten johdannaisten hinnoittelussa tai monimutkaisempien riskien mittaamisessa käytetään niin kutsuttuja Monte Carlo -menetelmiä. Niissä muodostetaan satunnaisesti suuri joukko mahdollisia toteumia tarkastellulle ilmiölle, joista otoksen keskiarvona saadaan estimaatti halutulle muuttujalle. Monte Carlo -menetelmien tehostamista pidetään yhtenä lupaavimmista kvanttisovelluksista, koska on osoitettu, että kvanttitietokonetta käyttäen estimointi voidaan laskea yhtä tarkasti neliöllisesti pienemmällä otoksella. Kvanttitietokoneet voivat siten vähentää merkittävästi tarvittavien simulaatiokierrosten määrää (Heinrich, 2001). Tämä on tärkeä edistysaskel, sillä klassisella laskennalla hinnoittelun tarkkuuden

5. Luonnollisen kielen käsittelyllä viitataan tekoälyratkaisuihin, joilla pystytään käsittelemään ja analysoimaan kielidataa, kuten esimerkiksi tieteellisiä artikkeleita tai uutisia.

parantaminen voi vaatia miljoonia tai jopa miljardeja Monte Carlo -simulointeja (Bouland et al., 2020). Tulevaisuudessa tällainen tehokkuusloikka voisi siten mahdollistaa jopa reaaliaikaisen johdannaisten hinnoittelun Monte Carlo -menetelmillä.

Portfolion optimointitehtävissä tarkoitus on minimoida portfolion riski samalla kun saavutetaan jokin tuottotavoite. Yksinkertaisimmillaan tehtävä voi olla suhteellisen helppo ratkaista, mutta laskennallinen vaikeus kasvaa heti kun tehtävään lisätään realistisempia rajoitteita, kuten esimerkiksi mahdollisuus myydä arvopapereita lyhyeksi. Rajoittamattomissa optimointitehtävissä kvanttialgoritmien on osoitettu pystyvän huomattaviin nopeusparannuksiin monissa eri tapauksissa (Rebentrost et al., 2018). Rajoitetuissa portfolion optimoimistehtävissä kvanttialgoritmien nopeushyödyt tulevat esiin esimerkiksi tapauksissa, joissa tehtävä supistetaan konveksiksi optimointitehtäväksi (Kerenidis et al., 2019). Vaikeisiin kombinatorisiin optimointitehtäviin sovelletaan yleensä likimääräisiä heuristisia ratkaisumenetelmiä. Kvanttitietokoneelle on kehitetty tällaisiin ongelmiin tehokkaampia kvanttiheuristiikkoja, jotka löytävät parempia ratkaisuja nopeammin ja jumittuvat huonoihin paikallisiin ratkaisuihin pienemmällä todennäköisyydellä.[6]

Koneoppimisella viitataan yleisesti tekoälyn osa-alueeseen, jossa pyritään opettamaan tietokoneita päättelemään aiempien tietojen perusteella. Rahoitusmarkkinoilla koneoppimista voidaan soveltaa esimerkiksi algoritmipohjaiseen kaupankäyntiin tai poikkeavien transaktioiden tunnistamiseen (katso myös Kolanovic et al., 2017). Kvanttiteknologialla tehostettu koneoppiminen on lupaava tutkimuskohde, sillä kvanttialgoritmit lupailevat monessa tapauksessa koneoppimiselle jopa eksponentiaalisesti nopeampaa laskentaa (Keredenis et al., 2017). Tällaiset sovellukset ovat kuitenkin vielä varsin monimutkaisia ja vaativat käytännössä sellaisia kvanttitietokoneratkaisuja, joita ei ole vielä olemassa[7].

Kansainvälinen keskuspankkiyhteisö seuraa aktiivisesti alan kehitystä ja on mukana ratkaisujen kehittämisessä

Kvanttiteknologian nopea kehitys ei ole jäänyt kansainväliseltä yhteisöltä huomaamatta. Huomion kohteena on erityisesti kvanttialgoritmien potentiaalinen vaikutus nykyisiin salausmenetelmiin, joihin rahoitusjärjestelmä tukeutuu vahvasti. Kvanttilaskennan on osoitettu pystyvän murtamaan nykyisten salausalgoritmien pohjana olevan julkisiin avaimiin perustuvan salauksen nk. Shorin kvanttialgoritmin avulla. Tämä myös vaarantaa tietoverkoissa suojattuna välitettyyn dataan perustuvien nykyisten järjestelmien turvallisuuden nk. store now, decrypt later -riskien kautta[8].

---

6. Rajattuihin käyttötarkoituksiin sopivilla kvanttijäähdyttimillä voidaan jo ratkaista niin sanottuja QUBO-formulointia noudattavia tehtäviä. Monia tunnettuja optimointitehtävämuotoja voidaan muuntaa QUBO-mallisiksi, ks. esimerkiksi (McMahon et al., 2022). Myös yleisempiä kombinatorisen optimoinnin kvanttiheuristiikkoja on esitetty (esimerkiksi Amaro et al, 2022).
7. Kvanttikoneoppimisen erityispiirre on, että se vaatii toimiakseen kvanttimuistia (nk. QRAM), jonka avulla suurempaa määrää dataa voitaisiin syöttää kvanttialgoritmeille. Tekniikkaa tähän ei ole vielä olemassa.
8. Suojatut tiedot voidaan teoriassa tallentaa nyt ja säilöä siihen asti, että salauksen purkaminen onnistuu kvanttitietokoneella.

Näiden uhkien takia Yhdysvaltojen kyberturvaviranomainen (CIS) on yhteistyössä kansallisen standardi- ja teknologiainstituutin (NIST) kanssa laatinut tiekartan jonka tarkoituksena on ohjeistaa organisaatioita valmistautumaan siihen asti, että kvanttikestävän salauksen standardit julkaistaan. Vastaavasti kansainvälinen valuuttarahasto (IMF) on peräänkuuluttanut rahoituslaitoksia aloittamaan varotoimenpiteiden implementoinnin (Deodoro et al., 2021), ja samoista syistä Yhdysvaltain keskuspankki nimesi äskettäin kvanttiteknologian nousevaksi uhaksi rahoitusmarkkinoiden yhtenäisyydelle ja luotettavuudelle (Board of Governors of the Federal Reserve System, 2023).

Työ kvanttiturvallisten ratkaisujen standardoimiseksi on jo pitkällä. Italian keskuspankki on tutkinut kvanttiturvallisia maksujärjestelmiä ja ehdottaa, että mm. tehokkaammilla satunaislukujen muodostamisen menetelmillä ja kvanttisalatulla avainten vaihdon menetelmillä (nk. *quantum key distribution*) voitaisiin lisätä järjestelmien kvanttiturvallisuutta. Kansainvälinen järjestelypankki (BIS) yhdessä Ranskan keskuspankin ja Saksan keskuspankin kanssa ovat Project Leap -projektissaan tutkineet millaisia uhkia kvanttilaskenta asettaa rahoitusdatalle ja millaisia uusia ratkaisuja tarvitaan, jotta rahoitusjärjestelmä olisi valmis kvanttiaikakauteen. Näissä ratkaisuissa nk. kryptografinen ketteryys[9] on tärkeässä asemassa.

Kvanttiteknologia voi myös tuoda uutta näkökulmaa sellaisiin rahoitusmarkkinoiden rakenteellisiin kysymyksiin, joissa nykyisiä markkinarakenteita on syntynyt tai suunniteltu olemassa olevan tekniikan kapasiteetin rajoituksien sanelemana. Esimerkki tällaisesta voisi olla maksamisen tai osakekaupankäynnin selvityksen infrastruktuurit. Kvanttilaskenta voi muuttaa tällaisten rajoitteiden sijaintia ja siten mahdollistaa muutoksia järjestelmien tai markkinoiden optimaalisissa rakenteissa. Tämä voi esimerkiksi suosia keskitetympiä rakenteita, joissa saadaan hyöty laajempien kokonaisuuksien optimoinnista

Suomen Pankki on aktiivisesti mukana kansainvälisessä yhteistyössä ja panostaa myös kotimaisen kvanttiteknologian kehityshankkeisiin osallistumalla esimerkiksi VTT:n koordinoiman kvanttiteknologian tutkimuskonsortion työhön.

Kirjallisuutta:

- Adam Bouland, Wim van Dam, Hamed Joorati, Iordanis Kerenidis, and Anupam Prakash. Prospects and challenges of quantum finance, 2020.
- Alexandre Ménard, Ivan Ostojic, Mark Patel, and Daniel Volz. A game plan for quantum computing, 2020.
- Board of Governors of the Federal Reserve System. Report to Congress: cybersecurity and financial system resilience report, 2023
- Christopher McMahon, Donald McGillivray, Ajit Desai, Francisco Rivadeneyra, Jean-Paul Lam, Thomas Lo, Danica Marsden, Vladimir Skavysh. Improving the Efficiency of Payments Systems Using Quantum Computing, 2022.
- Dylan A. Herman, Cody Googin, Xiaoyuan Liu, Alexey Galda, Ilya Safro, Yue Sun, Marco Pistoia, and Yuri Alexeev. A survey of quantum computing for

9. Kryptografisella ketteryydellä viitataan kykyyn siirtyä helposti salausalgoritmista toiseen, jos nyt standardoitavissa salaustuotteissa ilmenisi heikkouksia tai haavoittuvuuksia.

finance, 2022.
- Iordanis Kerenidis and Anupam Prakash. Quantum recommendation systems. Proceedings of the 8th Innovations in Theoretical Computer Science Conference, 2017.
- Iordanis Kerenidis, Anupam Prakash, Dániel Szilágyi. Quantum Algorithms for Portfolio Optimization, 2019.
- Jose Deodoro, Michael Gorbanyov, Majid Malaika, Tahsin Saadi Sedik. Quantum computing and the financial system: spooky action at a distance, 2021.
- Marko Kolanovic and Rajesh T. Krishnamachari. Big data and AI strategies: Machine learning and alternative data approach to investing, 2017.
- Michael Bogobowicz, Scarlett Gao, Mateusz Masiowski, Niko Mohr, Henning Soller, Rodney Zemmel, and Matija Zesko. Quantum technology sees record investments, progress on talent gap, 2023.
- Patrick Rebentrost, Seth Lloyd. Quantum computational finance: quantum algorithm for portfolio optimization, 2018.
- Stefan Heinrich. Quantum summation with an application to integration, 2002.
- Tucker Bailey, Soumya Banerjee, Christopher Feeney, and Heather Hogsett. Cybersecurity: Emerging challenges and solutions for the boards of financial-services companies, 2020.
- World Economic Forum. State of quantum computing; building a quantum economy, 2022.
- David Amaro, Carlo Modica, Matthias Rosenkranz, Mattia Fiorentini, Marcello Benedetti, Michael Lubasch, Filtering variational quantum algorithms for combinatorial optimization. 2022

Avainsanat

kvanttilaskenta, finanssimarkkinat, rahoitusmarkkinat, kubitti, koneoppiminen, kvanttiteknologia, optimointi, montecarlo, kvanttitietokone, innovaatio, tietoturva