TEADLASE PILGUGA

Kas kvanthäkkerid saavad ligi meie pangakontodele?

Peeter Saari

Kui ma veerandsajandi eest Tartu Ülikooli tulin ja hakkasin lugema kursust kvantarvutite alustest, oli kvantinformaatika buum maailma teaduskeskustes juba alanud. Nüüd teatas IBM, et nad on murdnud saja kvantbiti psühholoogilise barjääri, ehitades ülijuhtidel rekordilise 127-kvantbitise arvuti. Siiski sellega praktikas palju teha veel pole ja saavutus on eelkõige märgiline hüpe kvantinfotehnoloogia arengus. Millal see areng algas ja miks ta nii aeglane on?

Veel 1980ndate lõpus ei vaevanud informaatikud ja arvutiteadlased oma pead sellega, mis arvutis õigupoolest neid bitte-baite füüsiliselt kannab, ja kvantmehaanika oli neile täiesti terra incognita. Füüsikud omakorda suhtusid arvutitesse kui tööriista-abivahendisse. Kuid siis tulid paar end mõlemas valdkonnas kodus tundvat geeniust lagedale teoreetiliste uurimustega. Need näitasid, et kui oleks olemas kvantarvuti, siis sellele oleks käkitegu mitte ainult lahti muukida tavaarvutite jaoks murdmatud krüptokoodid, vaid sekunditega lahendada nii mõnigi ülesanne, millele ka kõige võimsam tavaarvuti kulutaks kuid. Arusaadavalt hakkasid teema vastu huvi tundma suurriikide teadagi missugused ametkonnad ning suurfirmad ja rahakraanid mastaapseks uurimistööks avanesidki. Sellele andsid hoogu ja hagu juurde veel kaks asjaolu.

Enne sajandivahetust olid suurpangad palganud tööle arvukalt füüsikuid usus, et uued, matemaatilise füüsika võrrandeid kasutavad meetodid lubavad paremini ennustada finantsturgude käitumist. Kui aga selgus, et neil turgudel kauplejate psühholoogia ja inimliku käitumise ettearvamatus kuni karjahüsteeriani välja on allumatu kuitahes keerulistele võrranditele, lasti pankadest lahti arvukalt füüsikadoktoreid. Viimased hõivasid aga informaatika ja kvantmehaanika vahelise siirdeala töökohad.

Tulemusena on tänaseks välja mõeldud hulk algoritme, mis kvantarvutil jooksutades lahendaks kiirelt tavaarvutite võimete piiril olevad probleemid. Toome näiteks otsinguülesande järjestamata kirjetega ja registrita andmebaasis, nagu on telefoniraamatust nime leidmine numbri järgi. On ilmne, et keskeltläbi tuleb otsitava leidmiseks läbi vaadata pool telefoniraamatut, st N/2 kirjet, kus N on telefoninumbrite arv. Kui andmebaas on keeruline ja N ületab miljardeid, muutub ka arvutiga otsingu aeg pikaks, sest see kasvab võrdeliselt Niga. Kvantarvutiga oleks otsinguaeg aga võrdeline ruutjuurega Nist ehk palju lühem.

Teiseks, sajandivahetuse paiku jõudis arvutiinseneridele pärale, et üha suurema arvu elektroonikaelementide tihepakkimisel kiipidesse-protsessoritesse on varsti piir ees. See tuleneb nii materjali kui ka elektrivoolu diskreetsest loomusest mikrotasandil. On ju mõistetav, et bitti kandev mälupesa saab koosneda kõige vähem ühest aineaatomist. Isegi meie moblades kulgevaid bitte ei saa pidada pideva elektrivoolu impulssideks, vaid neid tuleb käsitada väikese arvu

TEADLASE PILGUGA

elektronide kogumina. Diskreetsetest loenduvaist osakestest koosnev objekt käitub teisiti kui pidev.

Toome robustsevõitu analoogia. Meesterahvad on vast näinud innovaatilisemate WCde pissuaaride põhjas kärbse kujutist, mis meelitab pideva joa suunama ilmselt pissuaari parimale ja hügieenilisimale trajektoorile. Võrdluseks – kui tõenäone on lasta automaadist kõik kuulid märklaua kümnesse? Mikromaailma diskreetne loomus toob mängu kvantmehaanilise tõenäosuse koos kvantbitina toimiva mikrosüsteemi seisundite paljususe ja nende nn põimitusega.

Viimased annavadki kvantarvuteile nn kvantülimuslikkuse. IBMi 127-kvantbitise raaliga muidugi veel suuri ülesandeid lahendada ei anna. Paraku on kvantseisundid väga õrnad ja lagunevad kiiresti keskkonnaosakeste soojusliikumise n-ö pommirahe käes. Seepärast saab kvantarvuti töötada vaid teda jahutades võimalikult lähedale absoluutsele nullile (–273o C), mis nõuab vägevat krüotehnikat. Seejuures ikkagi suur osa kvantbittidest tuleb panna parandama arvutavates kvantbittides paratamatult tekkivaid vigu.

Need on põhjused, miks praktiliselt töötava kvantarvuti loomine on jäänud kümnendeiks silmapiirile ahvatlevalt küütlema. Siiski on IBMi ja paljude teiste uurimislaborite pingutused vilja kandmas – osaliselt juba täna, aga seda enam homme.

Seega võtame rahulikult – kvanthäkkerid ei tule veel niipea meie pangakoode murdma. Nagu meie tervist ohustab usk imerohtudesse ning vandenõuteooriatesse, nii ka meie pangakontodele lasevad telefoni- ja küberpätid ligi meie endi inimlikud nõrkused.

Kokkuvõttes tuleb tõdeda, et seni veel meie rumalus, kergeusklikkus ja kalduvus karjahüsteeriale ületab igapäevaelus mõjukuselt kvantülimuslikkuse.

Ilmunud ajalehes Postimees 4. detsembril 2021