KVANTARVUTI SISSEJUHATUS

Edmund Laugasson
IT Kolledž
Tallinna Tehnikaülikool

Arvutid täna

- klassikalised arvutid on võimaldanud hämmastavaid asju
  - internet: hajusteadmus (sarnane nt mesilastele)
  - seotus teiste eluvaldkondadega: alates elukorraldusest kuni meelelahutuseni välja

Arvutid täna

- kuigi arvutid võimaldavad täna hämmastavaid asju
- ei räägi me sageli neist asjadest, mida arvutid täna siiski veel teha ei suuda

Arvutid täna ebaõnnestuvad

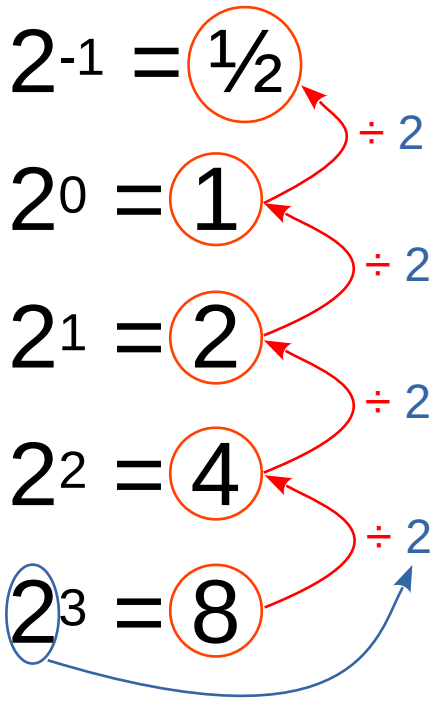
Paar näidet kus arvutid täna ebaõnnestuvad

- **optimeerimine** – soovitakse leida parim lahendus probleemile paljude teiste võimalike lahenduste hulgast
  - näiteks laud kuhu mahub istuma 10 inimest
  - mitu võimalust on neid inimesi erineva järjestusega (*permutatsioon*) istuma panna?
  - vastus on kümne faktoriaal: 10! = 3628800 erinevat järjestust
    - 10! = 10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1 ; **0! = 1**
    - https://www.taskutark.ee/m/permutatsioonid-ja-faktoriaal/

Allikas

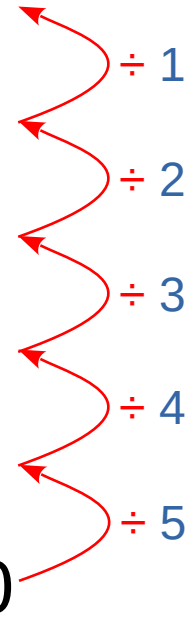
Miks 0! = 1 ?

- vastuseid tagasisuunas vaadates jagatakse iga kord kahega
  - $2^{-1} = ½$
  - $2^{0} = 1$
  - $2^{1} = 2$
  - $2^{2} = 4$
  - $2^{3} = 8$
  - jne...



Miks 0! = 1 ?

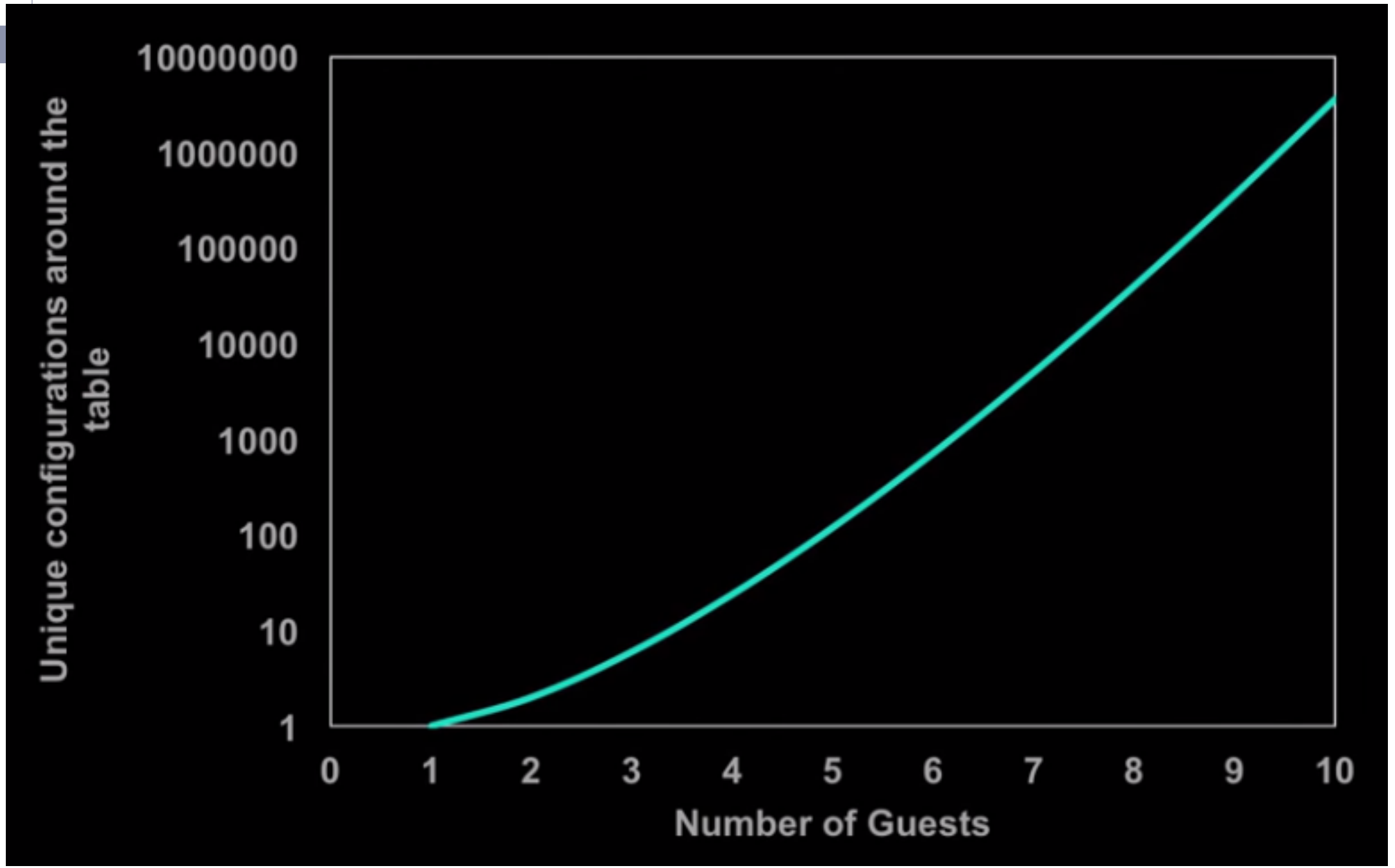
- vastuseid tagasisuunas vaadates jagatakse iga kord ühe võrra väiksema arvuga
  - 0! = 1
  - 1! = 1
  - 2! = 2
  - 3! = 6
  - 4! = 24
  - 5! = 120



Naturaalarvu n faktoriaal n! on n esimese positiivse täisarvu korrutis

Arvutid täna ebaõnnestuvad

- **optimeerimine**
  - seega 10 inimese laua taha istuma panemisel on ~3,6 miljonit erinevat võimalust
  - me kasutame sageli ligikaudseid väärtusi kiirema vastuse saamiseks
  - iga kord kui lisame ühe külalise lauda siis võimaluste arv erinevalt istuma panna kasvab eksponentsiaalselt
  - väikeste numbritega saame veel hakkama kuid suurematega enam mitte

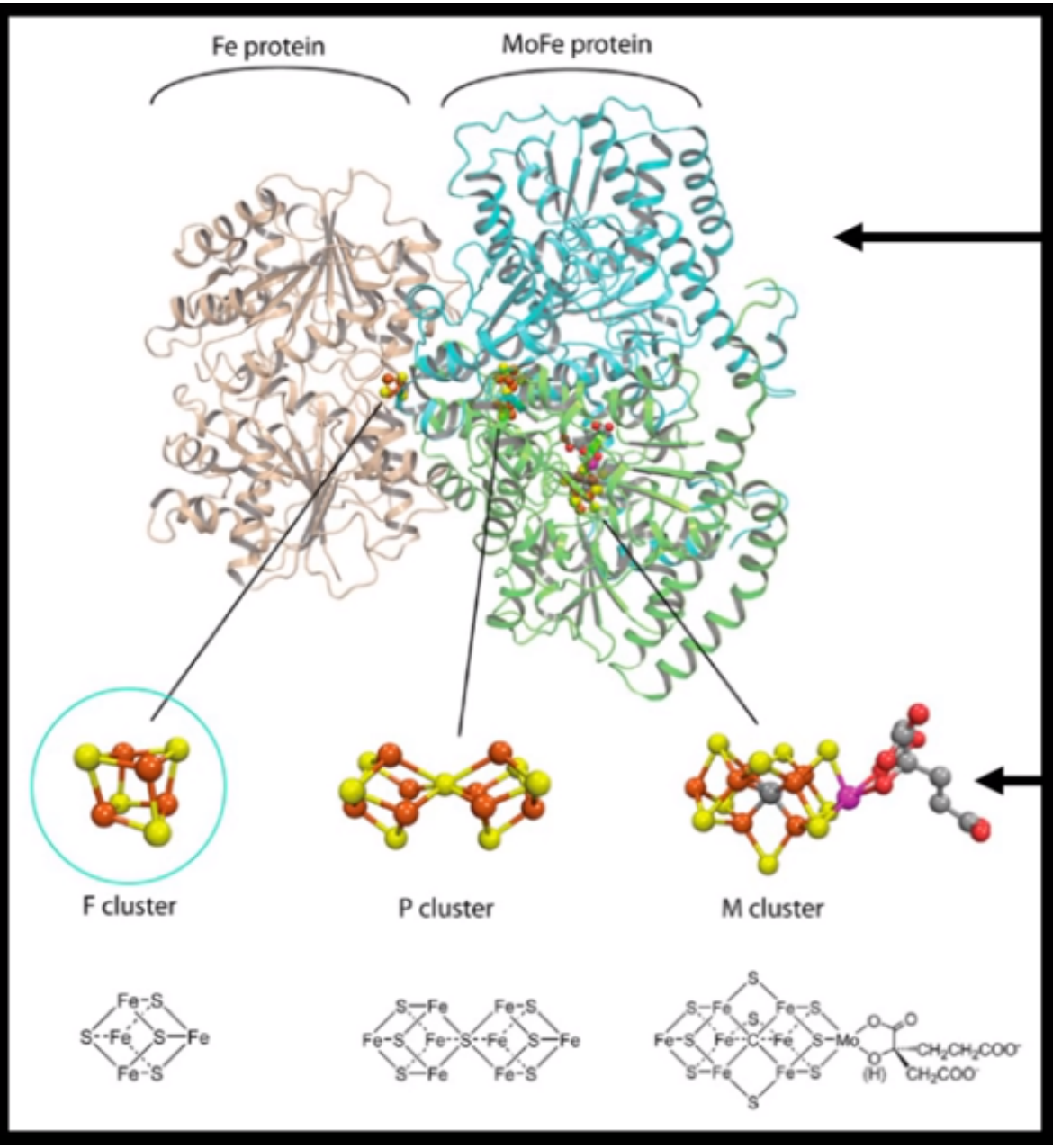


Allikas: *https://www.youtube.com/watch?v=S52rxZG-zi0*

Arvutid täna ebaõnnestuvad

- teine näide: keemia
  - nitrogenaasi ensüüm, mis on katalüsaator ammoniaagi loomisel, mis omakorda oluline väetiste, farmaatsiatoodete jne tootmisel
  - järgneval pildil on vasakul näha neli raua ja neli väävli aatomit – see on suurim raua-väävli molekul, mida tänased superarvutid simuleerida suudavad
  - põhjus: peab arvestama iga tõuke-, tõmbejõuga kõikide elektronide suhtes ja iga elektroni lisandudes tuleb kõik mõjuvad jõud uuesti arvutada - see number kasvab eksponentsiaalselt

Simulating this cluster is at the limit of classical computers



Nitrogenase enzyme involved in N_2 to NH_4 reaction

These regions are involved in different reaction stages

Iron sulfide clusters (Fe_xS_y) of different sizes.

Chem. Rev., **2014**, *114* (8), pp 4041–4062
DOI: 10.1021/cr400641x

Allikas: *https://www.youtube.com/watch?v=S52rxZG-zi0*

Arvutid täna ebaõnnestuvad

- nende probleemide ühine nimetaja on eksponentsiaalne kasvamine
- analoogne näide eksponentsiaalsest kasvust:
  - malelaua looja käest küsiti, mida ta soovib tasuks
  - ta soovis riisiterasid järgnevalt
  - malelaual on 64 ruutu
  - igale järgnevale ruudule kaks korda rohkem riisiteri kui eelmisele

Arvutid täna ebaõnnestuvad

- analoogne näide eksponentsiaalsest kasvust
  - alustame ühest riisiterast
  - kui jõuame 64 ruudule siis on $2^{64} \approx 1{,}85 \times 10^{19}$ (~18,5 kvintiljonit) riisitera!
  - 64 ei ole suur number kuid 2^{64} on juba väga suur
  - suured arvud riigiti erinevad - järgmisel slaidil

https://en.wikipedia.org/wiki/Names_of_large_numbers

Kümnendkohtade nimetused		
Kümnendkoht	Eestis, Venemaal, Prantsusmaal, USA-s	Suurbritannias, Saksamaal, Soomes
10^{6}	miljon	miljon
10^{9}	miljard	miljard
10^{12}	triljon	biljon
10^{15}	kvadriljon	biljard
10^{18}	kvintiljon	triljon
10^{21}	sekstiljon	triljard
10^{24}	septiljon	kvadriljon
10^{27}	oktiljon	kvadriljard
10^{30}	noniljon	kvintiljon
10^{33}	detsiljon	kvintiljard

Allikas: taskuteatmik A ja O

Tähis	Nimetus	Suurusjärk
Y	jotta-	$10^{24} = 1\,000\,000\,000\,000\,000\,000\,000\,000$
Z	zetta-	$10^{21} = 1\,000\,000\,000\,000\,000\,000\,000$
E	eksa-	$10^{18} = 1\,000\,000\,000\,000\,000\,000$
P	peta-	$10^{15} = 1\,000\,000\,000\,000\,000$
T	tera-	$10^{12} = 1\,000\,000\,000\,000$
G	giga-	$10^{9} = 1\,000\,000\,000$
M	mega-	$10^{6} = 1\,000\,000$
k	kilo-	$10^{3} = 1\,000$
h	hekto-	$10^{2} = 100$
da	deka-	$10^{1} = 10$
d	detsi-	$10^{-1} = 0{,}1$
c	senti-	$10^{-2} = 0{,}01$
m	milli-	$10^{-3} = 0{,}001$
µ	mikro-	$10^{-6} = 0{,}000\,001$
n	nano-	$10^{-9} = 0{,}000\,000\,001$
p	piko-	$10^{-12} = 0{,}000\,000\,000\,001$
f	femto-	$10^{-15} = 0{,}000\,000\,000\,000\,001$
a	ato-	$10^{-18} = 0{,}000\,000\,000\,000\,000\,001$
z	zepto-	$10^{-21} = 0{,}000\,000\,000\,000\,000\,000\,001$
y	jokto-	$10^{-24} = 0{,}000\,000\,000\,000\,000\,000\,000\,001$

Detsimaaleesliited SI mõõtühikute süsteemis

topeltühikuid ei kasutata, nt *µkg*

Allikas: taskuteatmik A ja O

Binaareesliited

Faktor	Nimi	Sümbol	Kordsus	SI süsteemis
2^{10}	kibi	Ki	$(2^{10})^1 = 2^{10}$	kilo: $(10^3)^1 = 10^3$ - tuhat
2^{20}	mebi	Mi	$(2^{10})^2 = 2^{20}$	mega: $(10^3)^2 = 10^6$ - miljon
2^{30}	gibi	Gi	$(2^{10})^3 = 2^{30}$	giga: $(10^3)^3 = 10^9$ - miljard
2^{40}	tebi	Ti	$(2^{10})^4 = 2^{40}$	tera: $(10^3)^4 = 10^{12}$ - triljon
2^{50}	pebi	Pi	$(2^{10})^5 = 2^{50}$	peta: $(10^3)^5 = 10^{15}$ - kvadriljon
2^{60}	eksbi	Ei	$(2^{10})^6 = 2^{60}$	eksa: $(10^3)^6 = 10^{18}$ - kvintiljon

Binaareesliited informaatikas
http://en.wikipedia.org/wiki/Binary_prefix
https://dl.acm.org/citation.cfm?id=1822591

Detsimaaleesliited teistes reaalteadustes:
https://www.taskutark.ee/m/kordsed-uhikud/
https://www.taskutark.ee/m/tahised-ja-mootuhikud/
http://et.wikipedia.org/wiki/%C3%9Chikute_detsimaaleesliited

Arvutid täna ebaõnnestuvad

- analoogne näide eksponentsiaalsest kasvust
  - kui 1 riisitera kaalub ~0,1g siis teeb see kokku (1,85x10^{19}x0,1)÷(1000x1000) ≈ 1844674407370,96 tonni ≈ 1844674,40737096 mln tonni riisi
    (1 tonn = 1 Mg megagramm ehk miljon grammi: 1000x1000)
  - maailmatoodang
    - 2016.a 741 mln tonni
    - 1844674,40737096÷741 ≈ 2489,44 korda rohkem

http://ricepedia.org/rice-as-a-crop/rice-productivity
https://en.wikipedia.org/wiki/Rice#Production
https://www.statista.com/topics/1443/rice/

Arvuti

- programmeeritav masin, kaks peamist omadust
  - arvuti reageerib kindlaksmääratud käskudele alati kindlal viisil
  - arvuti suudab tegutseda etteantud käskude jada ehk programmi alusel
- tänapäeval on arvutid elektroonilised ja digitaalsed
- ajalooliselt on tuntud ka mehaanilised ja analoogarvutid

Arvuti

- mikroprotsessoriga (CPU *Central Processing Unit*) arvuti saab aru vaid teda läbivatest elektrilistest signaalidest
- kui juhtmes on vool siis on loogikalüliti ehk trigeri väärtus 1 ja kui ei ole siis 0
- seega töötavad mikroprotsessoriga arvutid kahendsüsteemis (*binary system*)

Arvuti

- signaali 1 pinge väärtuseks on tavaliselt 5V
- arvutis on kasutusel kahte tüüpi alalispinget
  - 5V elektroonika juhtimiseks
  - 12V mootorite juhtimiseks (kõvaketas, optilise seadme sahtel, ventilaatorid jms)
- tegemist on alalisvooluga

Kvantarvuti

- kasutab informatsiooni töötluseks kvantmehaanika fenomene, näiteks superpositsiooni (*superposition*) ja põimumist (*entanglement*), et andmeid muuta
- kvantarvuti erineb tavalisest transistoritel põhinevast arvutist kuna tal on võime teostada tehteid tohutu suure paralleelsuse astmega
- IBM’i teadlase selgitused eri keerukustasemetel https://www.youtube.com/watch?v=OWJCfOvochA

https://heureka.postimees.ee/3983689/peeter-saari-jargmise-digirevolutsiooni-teeb-kvant-uleolek

Kvantarvuti

- superpositsiooni on nimetatud ka kvantüleolekuks (*quantum supremacy*), kvantparallelismiks
- Suurim tehniline probleem kvantarvuti valmisehitamise ees on kvantbiti õrnus. Vähimgi mõjutus, näiteks kas või kõike läbistav kosmiline kiirgus, rikub tema kvantoleku – just selle, kus ta on korraga seisundis 1 ja 0. Mida rohkem kvantbitte, seda kiirem-tõenäosem on nende ühise kvantseisundi lagunemine.

https://heureka.postimees.ee/3983689/peeter-saari-jargmise-digirevolutsiooni-teeb-kvant-uleolek
https://www.fyysika.ee/?p=4003
https://arxiv.org/abs/1203.5813 - *quantum supremacy*

Kvantarvuti

- Kvantprotsessoriga (QPU *Quantum Processing Unit*) kvantarvutites kasutatavad kvantlülitid (kvanttrigerid) töötavad superpositsiooni meetodil
- samaaegselt on võimalik nii 1 kui 0 positsioon - superpositsioon

Kvantarvuti - superpositsioon

- Lihtsustatult öeldes:
  - 1 kvantbitine (*qubit*) süsteem võimaldab kirjeldada kahte kvantolekut ($2^1 = 2$)
  - 2 kvantbitti võimaldab kirjeldada $2^2 = 4$ kvantolekut (astendaja on kvantbiti väärtus)
  - 3 kvantbiti korral juba $2^3 = 8$ kvantolekut
  - 2000 kvantbiti korral juba $2^{2000} = \sim 1{,}15 \times 10^{602}$ kvantolekut
  - seega on siin palju rohkem olekuid kui vaid 0 ja 1

Kvantarvuti - superpositsioon

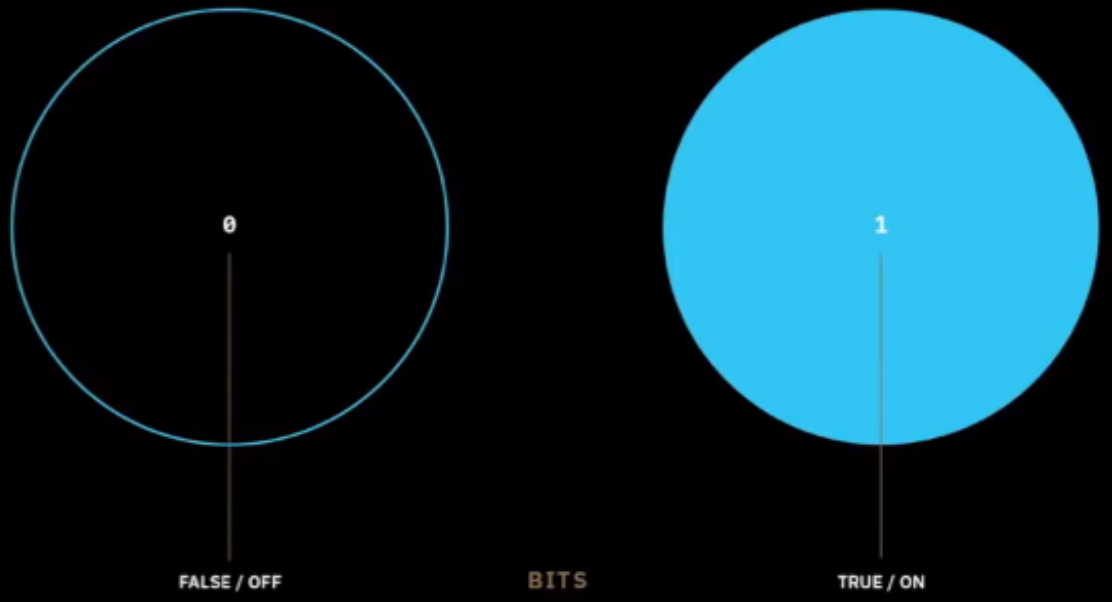
- Lihtsustatult öeldes:
  - superpositsioonis on samaaegselt 0 ja 1
  - mingi tõenäosusega toimub valik siis kui kvantbiti seisundit välja loetakse
  - analoogia: iga kohtunik on aus/ebaaus – üks neist alternatiividest realiseerub siis kui pistist pakutakse

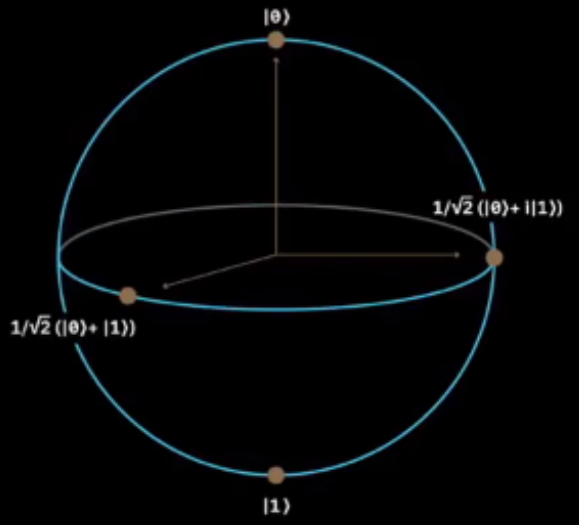
https://www.fyysika.ee/?p=4003

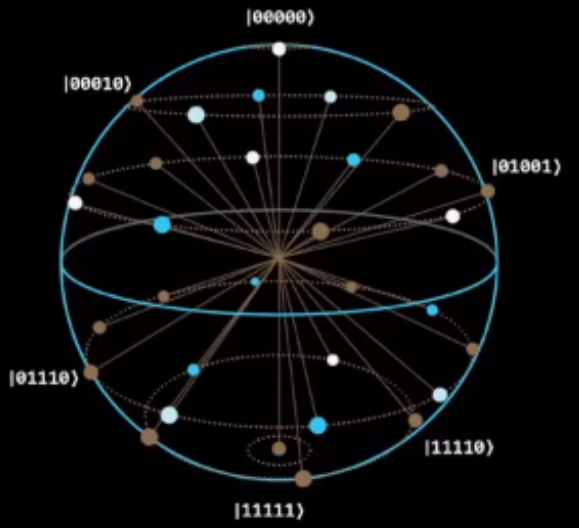
Why is quantum different?

1. Superposition

N qubits
2^N paths







Classical states

Quantum states

Allikas: *https://www.youtube.com/watch?v=S52rxZG-zi0*

paremal: 5 kvantbiti 32 (2^5) olekut

Kvantarvuti - põimumine

- Põimumine, põimolek ehk (kvant)põimitus on kahe või enama keha kvantolek, kus ei ole võimalik määrata süsteemi moodustavatest kehadest üksiku kvantolekut, isegi kui kehad on ruumiliselt eraldatud.
- Liitsüsteemi osad ehk komponendid on põimunud, kui liitsüsteemi olekufunktsioon pole avaldatav komponentide lainefunktsioonide korrutisena, vaid niisuguste korrutiste superpositsioonina. Tänu põimumisele võib kahe teineteisest määramata kaugusel asuva punkti vahel esineda korrelatsioon.

https://en.wikipedia.org/wiki/Quantum_entanglement
https://et.wikipedia.org/wiki/P%C3%B5imumine

Kvantarvuti - põimumine

- Einstein ei tahtnud põimumist uskuda, sest selle nähtuse puhul liigub info valgusest kiiremini. Sellepärast seletas ta põimumist varjatud parameetritega, mis on põimunud osakestel ühesugused ja mille järgi osakesed käituvad. Seda võib mõnes mõttes võrrelda ka algoritmidega informaatikas.
- Anton Zeilingeri korraldatud katses mõjutas ühes punktis tehtud otsustus silmapilkselt 144 kilomeetri kaugusel asuvat punkti, mis oli seotud põimumisega.

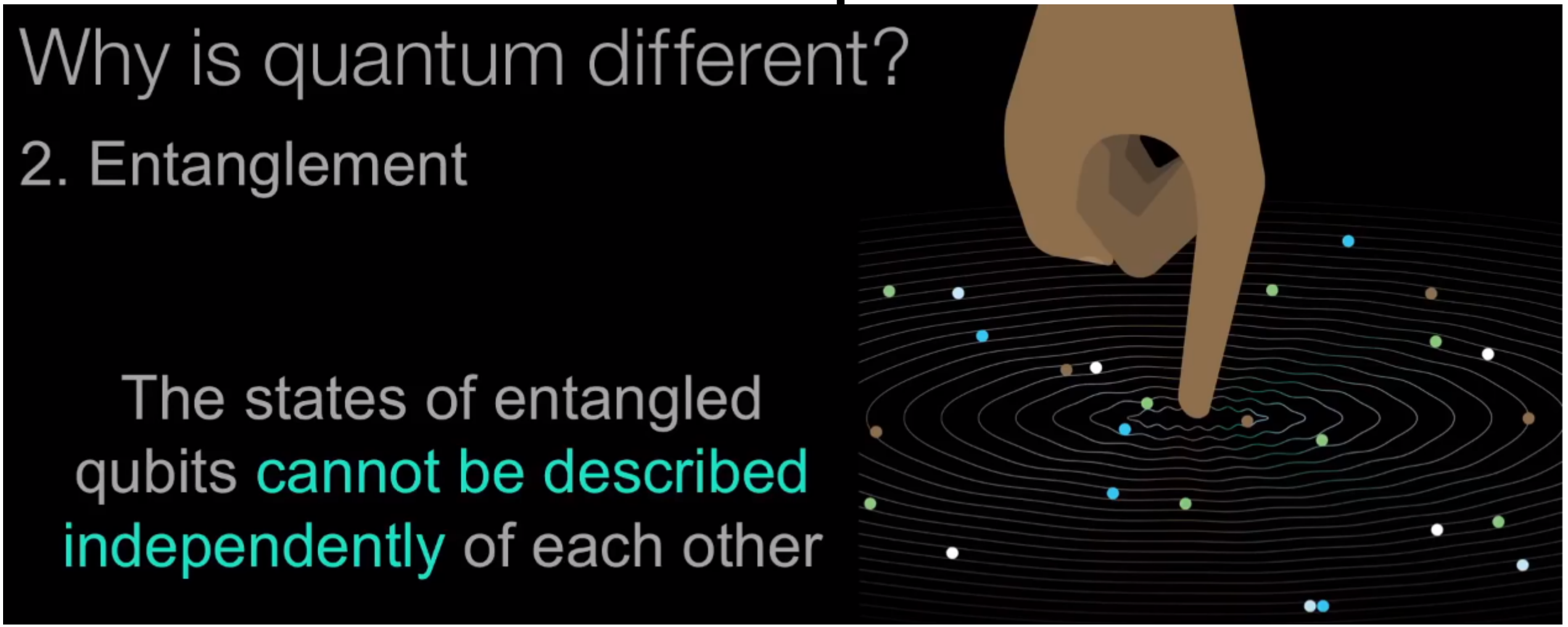
https://en.wikipedia.org/wiki/Quantum_entanglement
https://et.wikipedia.org/wiki/P%C3%B5imumine

Kvantarvuti - põimumine

- lühidalt:
  - omavahel põimolekus kvantbittide paaril neist ühelt seisundi väljalugemine määrab justkui ülevalguskiirusega ära teise kvantbiti oleku lugemi

https://www.fyysika.ee/?p=4003

Kvantarvuti - põimumine



näiteks: 2 kvantbitti põimitakse kokku: mõõtes ühte ütleb meile, mis juhtub kui mõõdame teist

Allikas: *https://www.youtube.com/watch?v=S52rxZG-zi0*

Kvantolek

- **Kvantolek** on kvantmehaanikas osakeste süsteemi matemaatiline kirjeldus väljendamaks elementaarosakeste omadusi.
- Kui klassikalises mehaanikas on mingi keha kirjeldamiseks oluline teada tema asukohta ja impulssi (millest on võimalik leida keha mass ja kiirus), siis kvantmehaanikas pole asukoht ja impulss enam korraga täpselt kirjeldatavad. Kvantmehaanikas kasutatakse osakese kirjeldamiseks kvantarve. Kvantarvud väljendavadki osakese olekut ja omadusi.

https://et.wikipedia.org/wiki/Kvantolek

Kvantarv

- **Kvantarv** on süsteemi olekut iseloomustav väärtus kvantmehaanikas. Kvantarvu eripäraks on tema diskreetsus (mittepidevus). See tähendab, et iga järgmine kvantarvu väärtus erineb eelmisest kindla suuruse ehk kvandi võrra.

https://et.wikipedia.org/wiki/Kvantarv

Kvant

- **kvant** – füüsikalise suuruse vähim jagamatu hulk
- Füüsikas on **kvant** (ladina sõnast *quantum* '*kui palju, kui suur*') füüsikaline objekt, mis tekib süsteemi üleminekul ühest olekust teise, kui selle süsteemi olekud vastavad teatud füüsikalise suuruse (enamasti energia) diskreetsetele väärtustele.
- Näiteks elektroni energia aatomis on kvantiseeritud. Kui elektron läheb üle madalama energiaga energianivoole, siis kiiratakse kvant, ja kui toimub üleminek kõrgema energiaga energianivoole, siis neelatakse kvant. Sellise kvandi energia on vastavate energianivoode energiate vahe.

https://et.wikipedia.org/wiki/Kvant
https://et.wikipedia.org/wiki/Kategooria:Kvantf%C3%BC%C3%BCsika
https://en.wikipedia.org/wiki/Category:Quantum_information_science
https://en.wikipedia.org/wiki/Category:Quantum_mechanics

Miks kvantarvuti aitab?

- superpositsiooni meetod – kahe oleku asemel on oluliselt rohkem olekuid
- põimimine on teine omadus peale superpositsiooni, mis annab vajalikku kvantinfot
- see kõik kokku muudab totaalselt seda kuidas me algoritme käivitame

Miks kvantarvuti aitab?

- näiteks optimeerimise ülesanne: 10 inimese paigutamisel laua äärde on ~3,63 miljonit võimalust
  - klassikaliselt tuleb iga võimalust individuaalselt kaaluda ja võrrelda
  - kvantarvuti: võtame kvantbitid, viime need superpositsiooni olekusse koos kõikide võimalike olekutega ja sätetega ning leiame põiminguid ja läbi selle tohutut paralleelsust kasutades kiire lahenduse

Miks kvantarvuti aitab?

- kui me sisestame oma probleemi kvantarvutisse
  - programmeerime iga oleku jaoks tema faasi – ligipääsu kvantsfääri keskele
  - kui võnge on faasis siis on olemas amplituud
  - vastandfaasis võnge tühistab
  - täpselt sama toimub aktiivse mürasummutusega kõrvaklappidega – tekitatakse vastandfaasis müra, et summutada väliseid helisid

Miks kvantarvuti aitab?

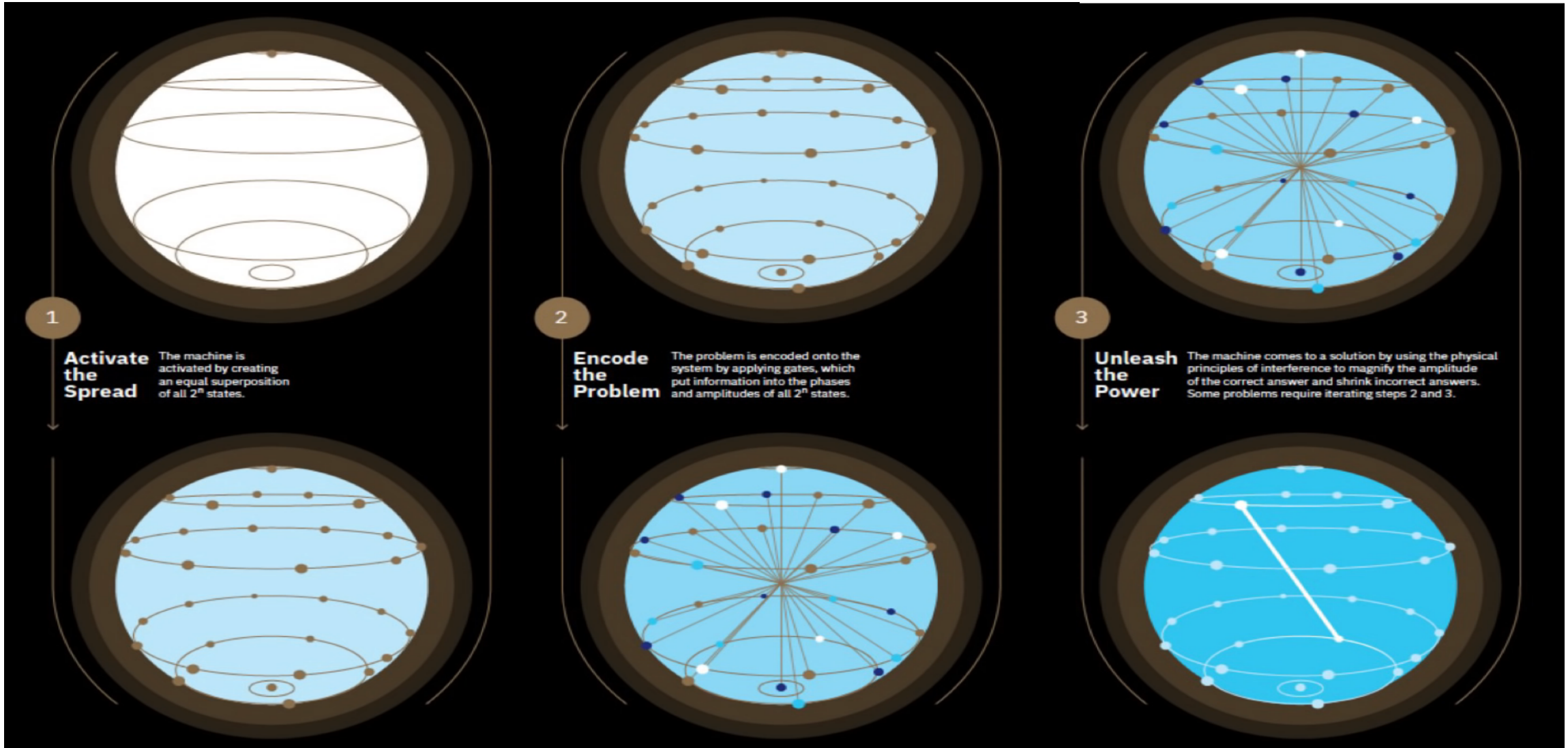
- kui me sisestame oma probleemi kvantarvutisse
  - programmeerides iga oleku jaoks tema faasi – ligipääsu kvantsfääri keskele
  - seejärel kasutatakse interferentsi (liituvate lainete vastastikune mõju) – võimendatakse mõningaid vastuseid ja katkestatakse teisi
  - lõpuks jõutaksegi lahenduseni
  - see on täiesti teisiti kui seni arvutid on probleeme lahendanud

1) Aktiveerige levik
Masin on aktiveeritud kui kõikide kvantbittide olekute võrdsed superpositsioonid on loodud

2) Kodeeri probleem
Probleem on sisestatud kui on toimiv loogikavärav, mis paneb info kõikide kvantbittide olekute faasidele ja amplituudidele

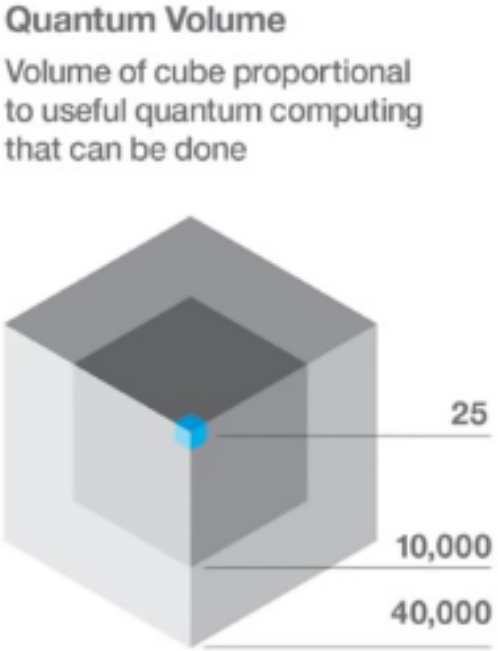
3) Vabasta võimsus
Masin leiab lahenduse kasutades interferentsi suurendab õige vastuse amplituudi ja kahandab vale oma. Mõned probleemid vajavad esimese 2 sammu kordamist.

Allikas: *https://www.youtube.com/watch?v=S52rxZG-zi0*



Mis veel on oluline?

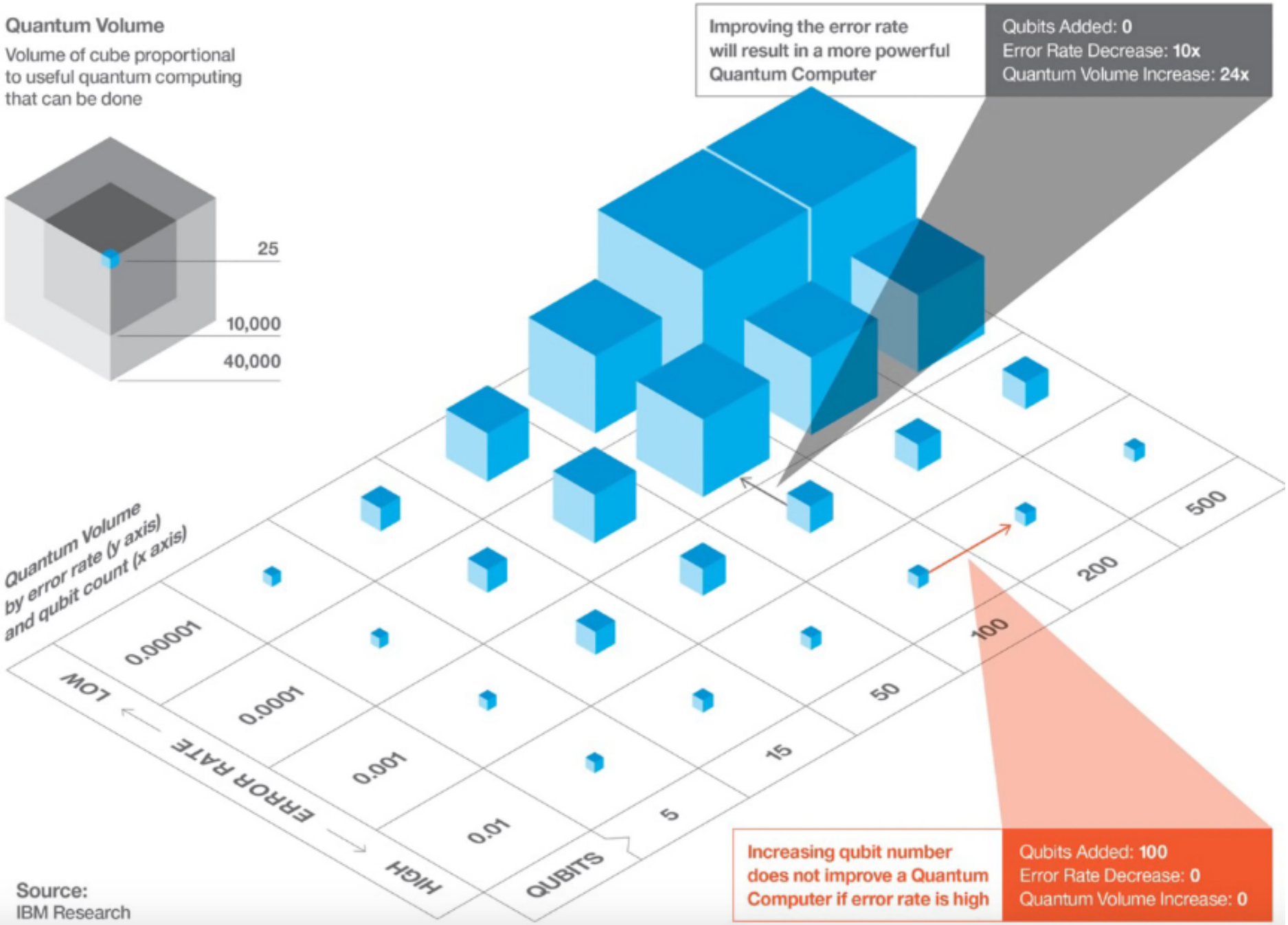
- lisaks kvantbittidele on oluline ka veakindlus
- *Quantum Volume* – arvestab kvantolekute ja nende veakindlusega iga operatsiooni täpsuse juures, samuti palju operatsioone vajatakse konkreetse probleemi lahendamiseks. Sisuliselt probleemi maht, mida kvantarvuti suudab uurida.



https://www.youtube.com/watch?v=S52rxZG-zi0

A Quantum Computer's power depends on more than just adding qubits

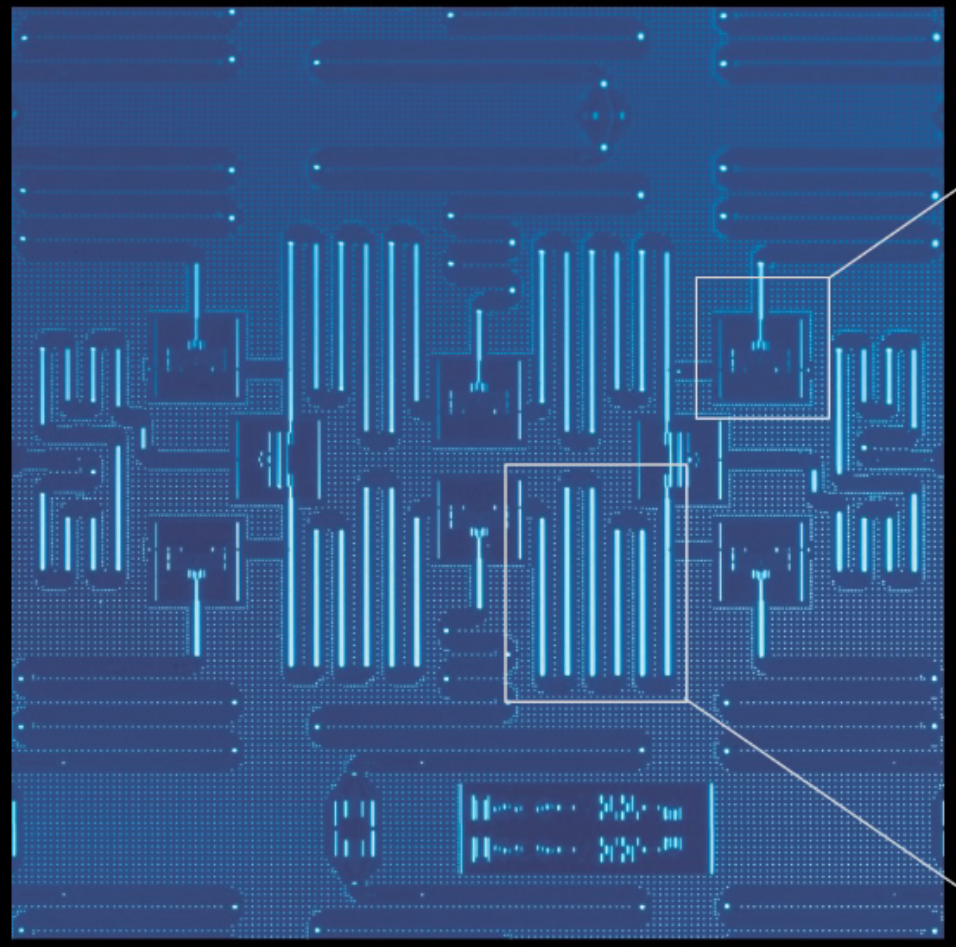
If we want to use quantum computers to solve real problems, they will need to explore a large space of quantum states. The number of qubits is important, but so is the error rate. In practical devices, the effective error rate depends on the accuracy of each operation, but also on how many operations it takes to solve a particular problem as well as how the processor performs these operations. Here we introduce a quantity called **Quantum Volume** which accounts for all of these things. Think of it as a representation of the problem space these machines can explore.



https://www.youtube.com/watch?v=S52rxZG-zi0

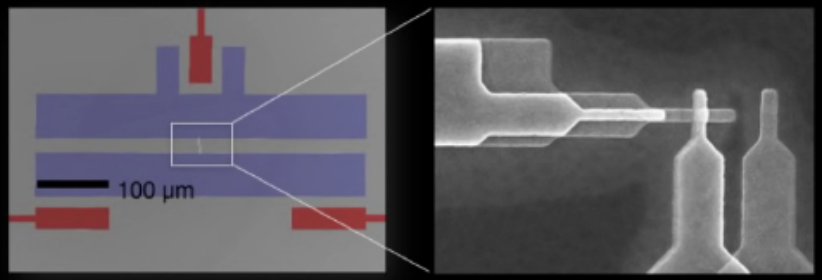
Kuidas kvantarvutit ehitada?

kvantkiibi tasandil vaade



Qubit → behaves like an artificial atom!

kvantmehhaanikale alluvad kvantbitid kui tehisaatomid



Superconducting Josephson Junction

0.015 Kelvin – colder than space!

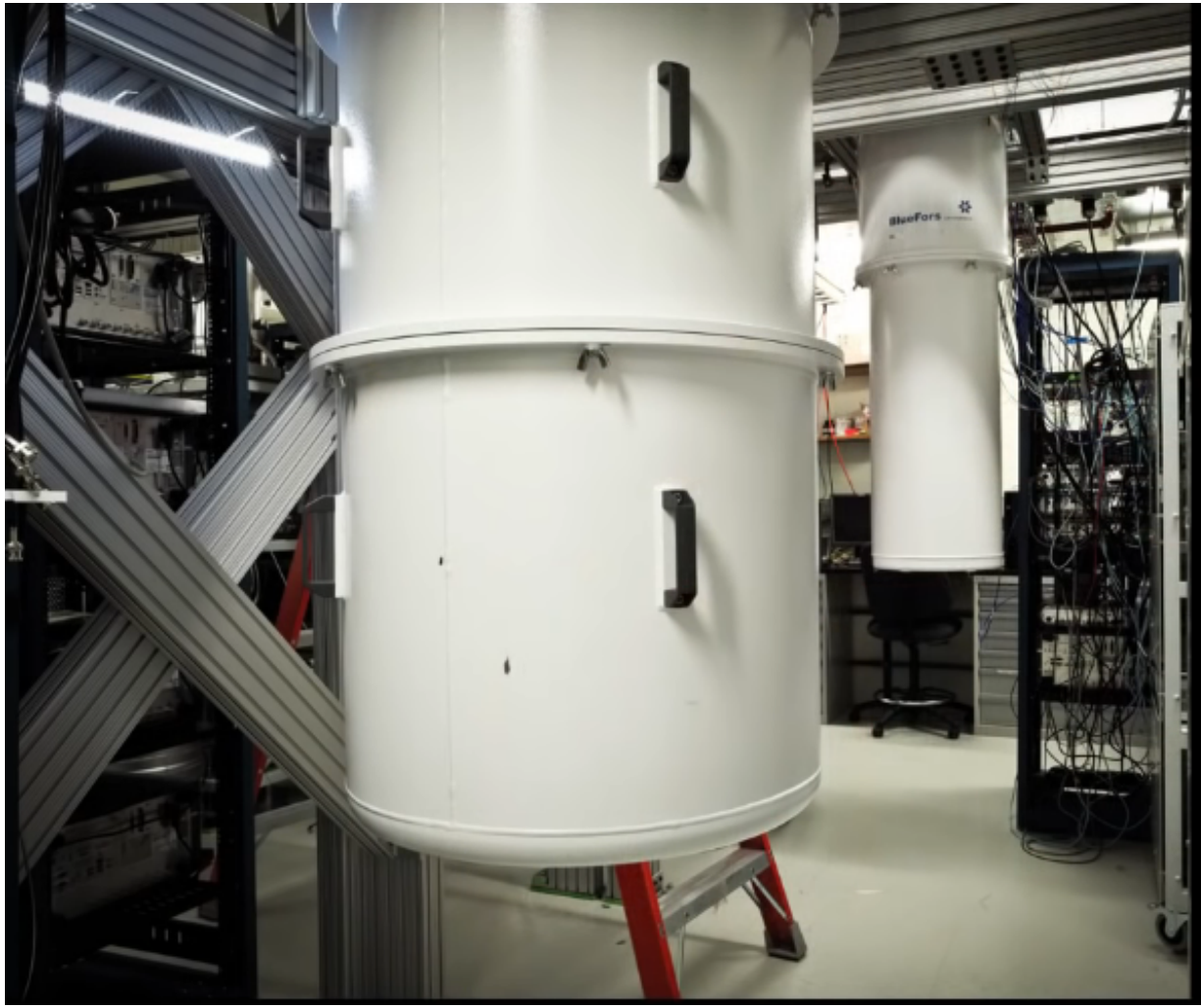
ülijuhtivad Josephsoni ühendused seotud mikrolaine resonaatoritega - adresseerivad ja paaritavad kvantbitte

Microwave resonator – address and couple the qubits

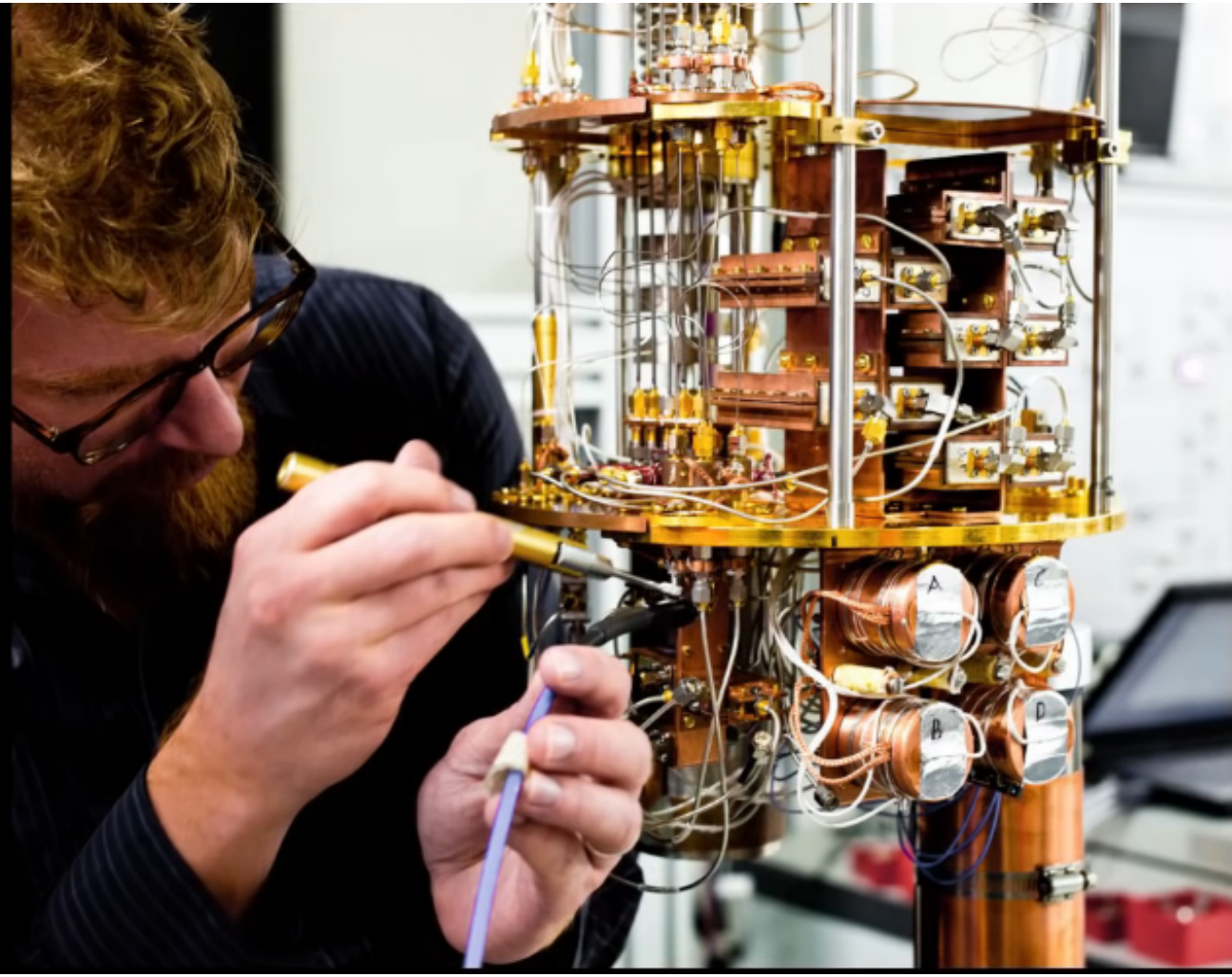
https://www.youtube.com/watch?v=S52rxZG-zi0

Mikrolaine kaablid ühendatud krüogeenilises (3He/4He) külmkambris, mis võimaldavad kvantbitte adresseerida ja paaritada

https://www.youtube.com/watch?v=S52rxZG-zi0
https://en.wikipedia.org/wiki/Dilution_refrigerator



krüogeeniline külmkamber (*dilution refrigerator*)

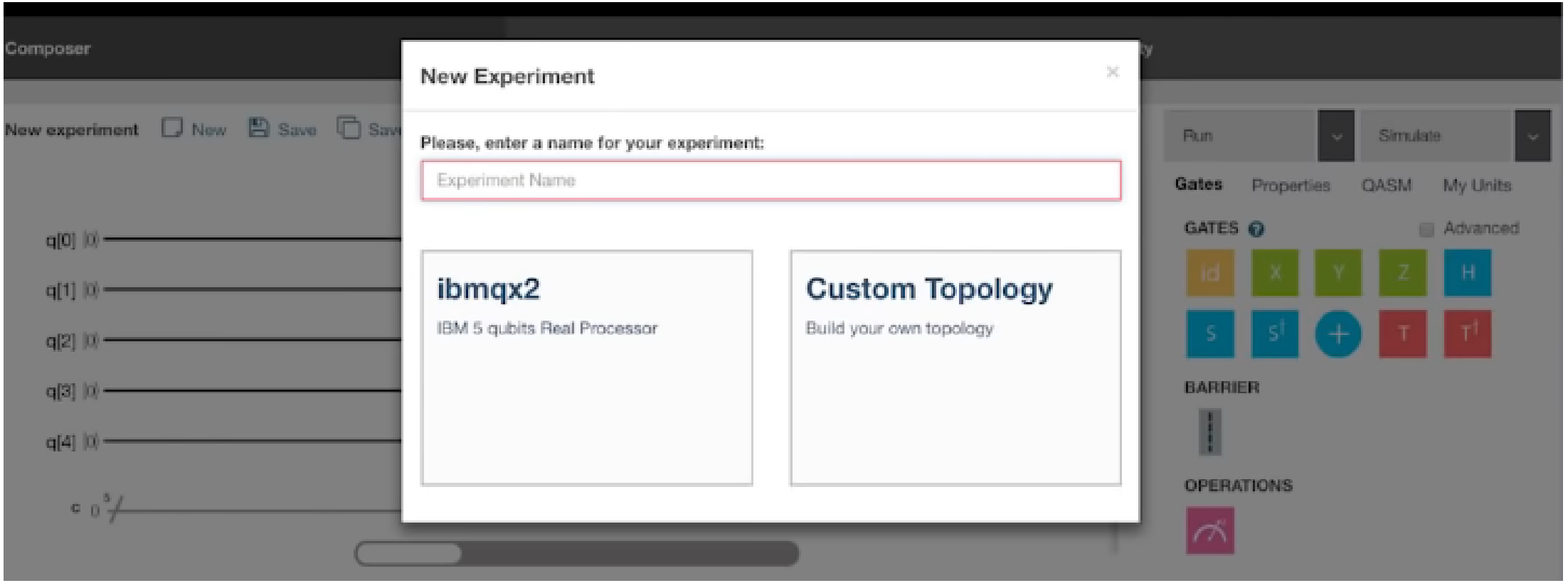


kvantsöötja (*quantum feeder*)

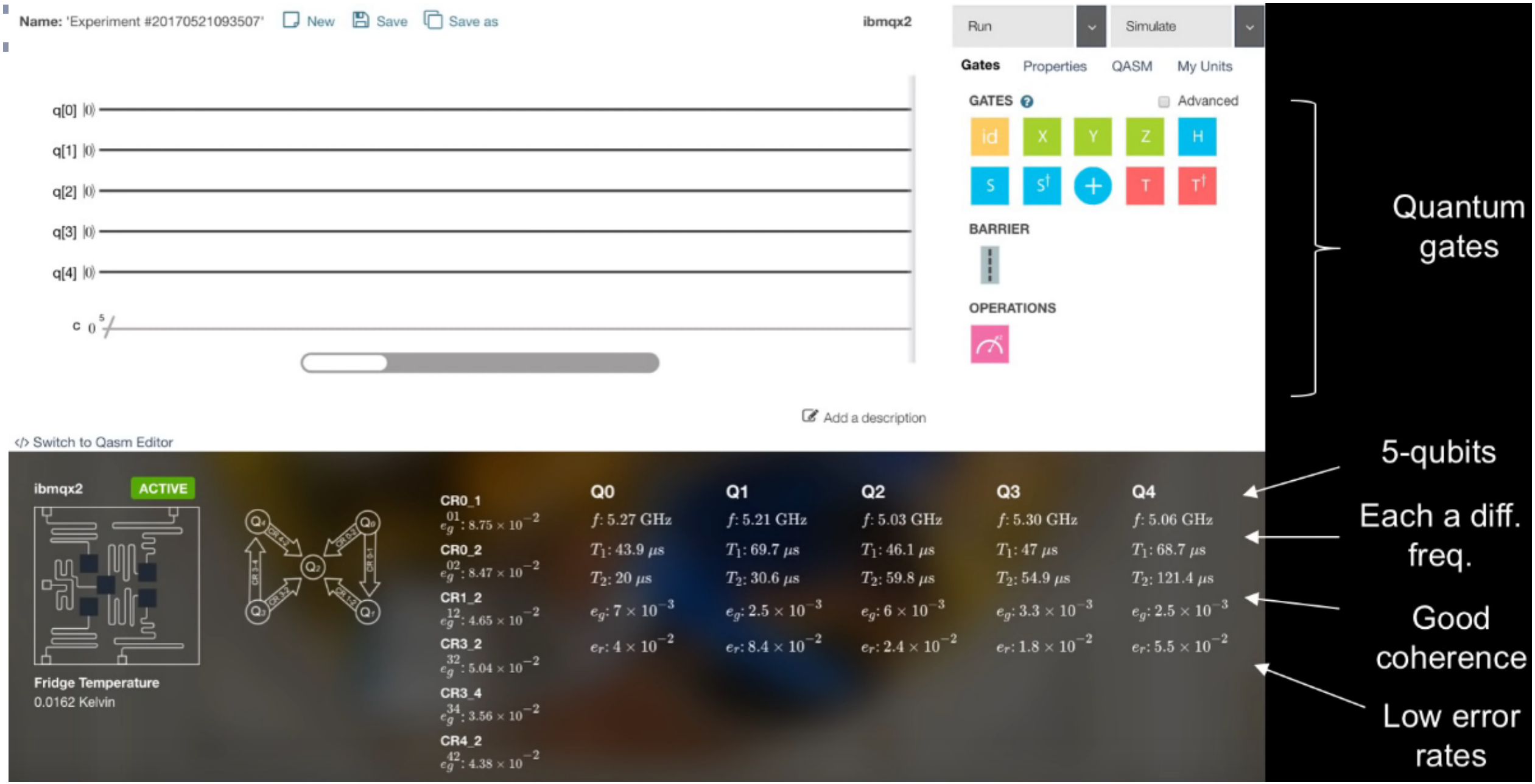
https://www.youtube.com/watch?v=S52rxZG-zi0
https://en.wikipedia.org/wiki/Dilution_refrigerator

Kvantarvuti veebis (IBMi näide)

- https://quantumexperience.ng.bluemix.net/

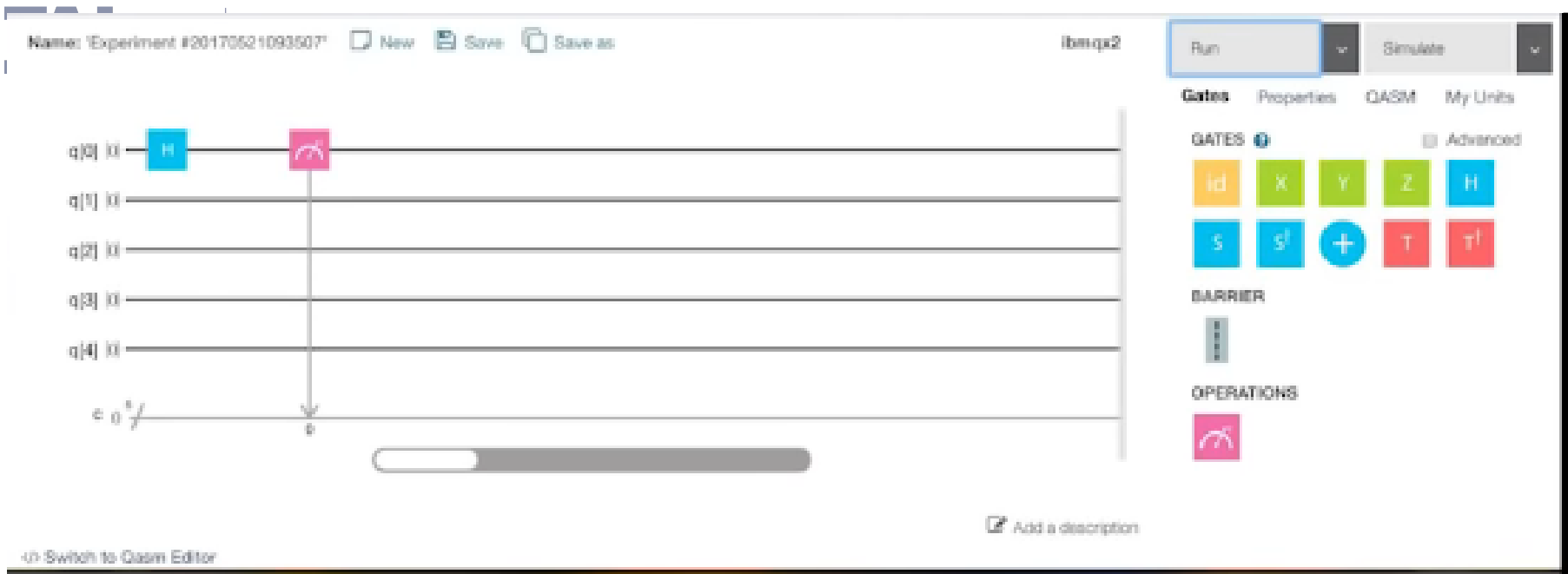


https://www.youtube.com/watch?v=S52rxZG-zi0



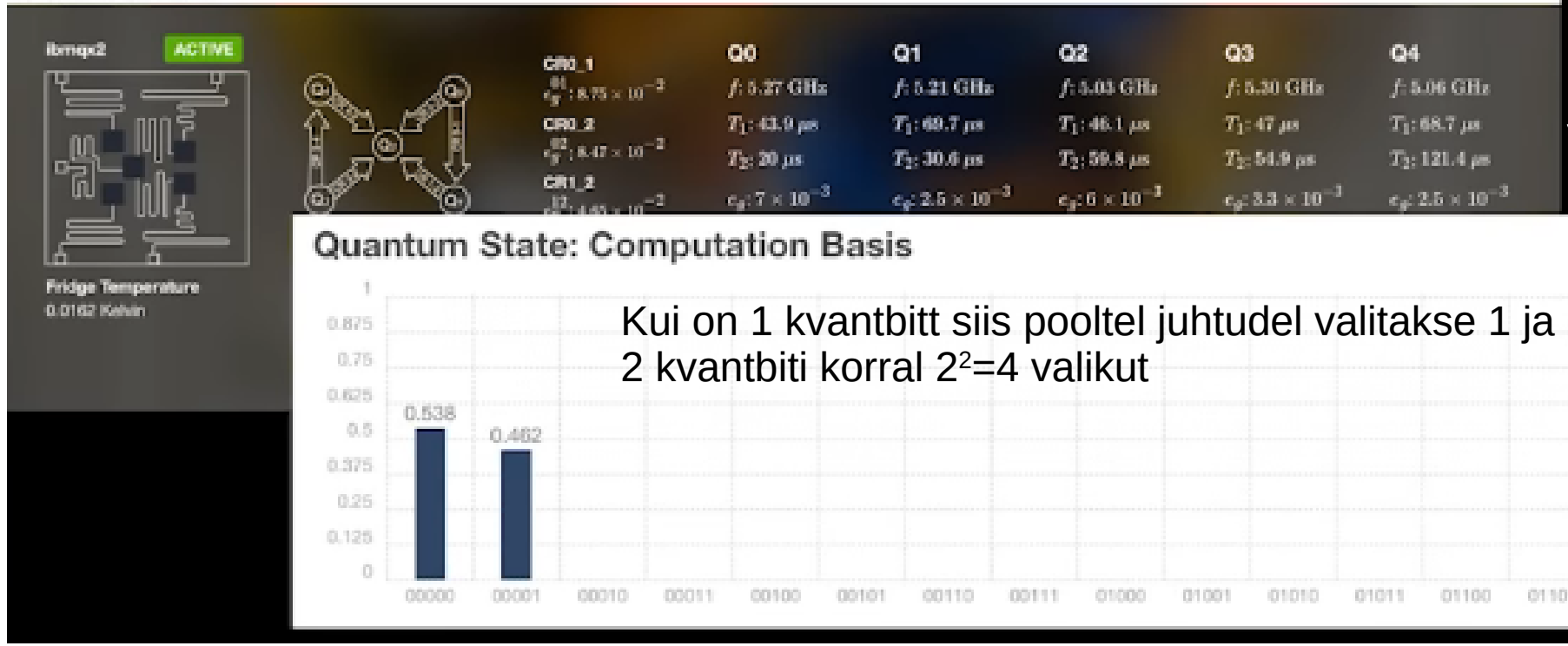
Mustad ristkülikud joonisel ongi kvantbitid, mis ühendatud mikrolaine resonaatoritega.

Infot kvantbittide kohta, sh sidususaeg (*coherence time*) – kaua tehete tegemiseks vajalik kvantinfo säilib enne kui sidusus kaob (50..100 ms).



Loome superpositsiooni, lohistades nt H-värava esimesele joonele, mis esitab 1.kvantbitti ja seejärel mõõtmine.

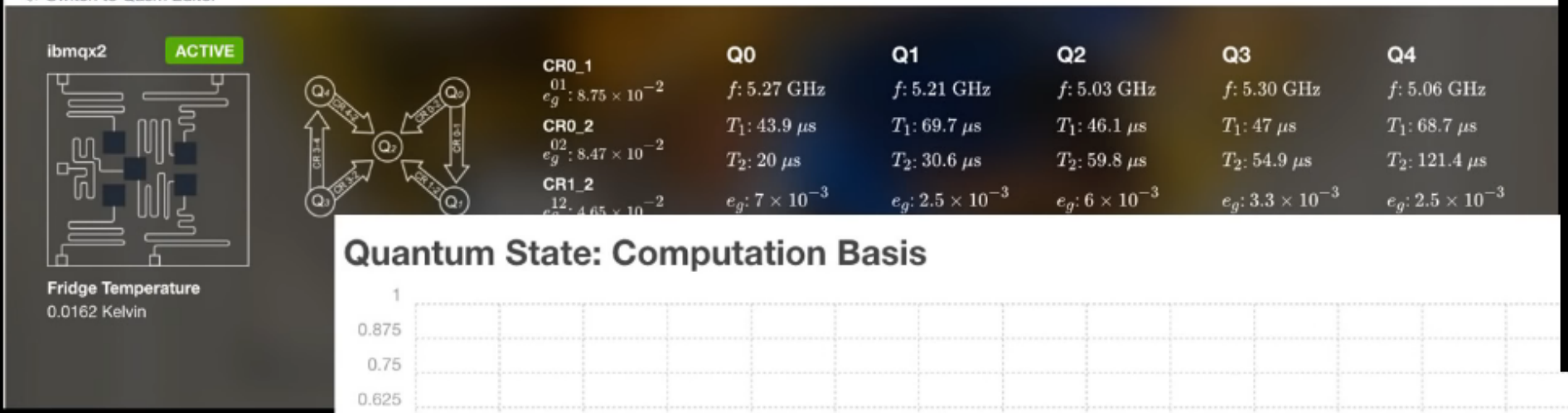
H-värav: Hadamard'i värav

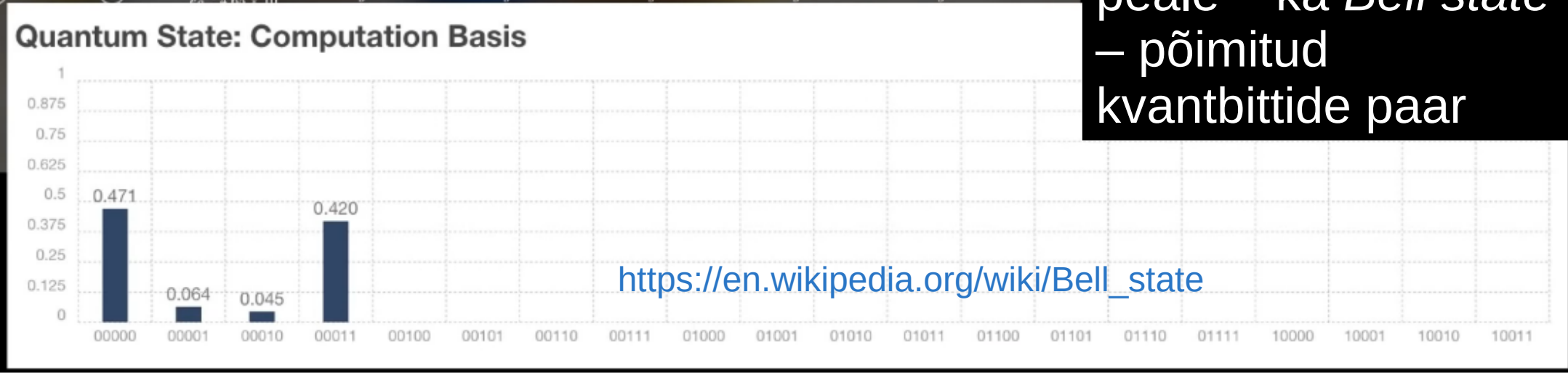


Kui on 1 kvantbitt siis pooltel juhtudel valitakse 1 ja pooltel 0.
2 kvantbiti korral 2^2=4 valikut

https://www.youtube.com/watch?v=S52rxZG-zi0

https://www.quantum-inspire.com/kbase/hadamard/





Põimimise (*entanglement*) loomine. Peale H-väravat lisati põimimisvärav (*CNOT gate*) – kui kvantbitt mõõdetakse olema 0 siis ära tee midagi ja kui 1 siis muuda ka teine kvantbitt 1 peale – ka *Bell state* – põimitud kvantbittide paar

https://en.wikipedia.org/wiki/Bell_state

Huvi korral võimalus tutvuda kvantalgoritmidega, nt Grover’i algoritm – kvantinterferents (liituvate lainete vastastikune mõju), mis võimendab amplituudi

Full User Guide

For those who have some prior experience with Linear Algebra or Quantum Computing

Section IV

Quantum Algorithms

A more profound look into the wonderful world of quantum, diving head-first

Section V

Quantum Error Correction

Fighting errors with entanglement.

Section VI

The Real Nitty-Gritty Details

Users enter at your own risk.

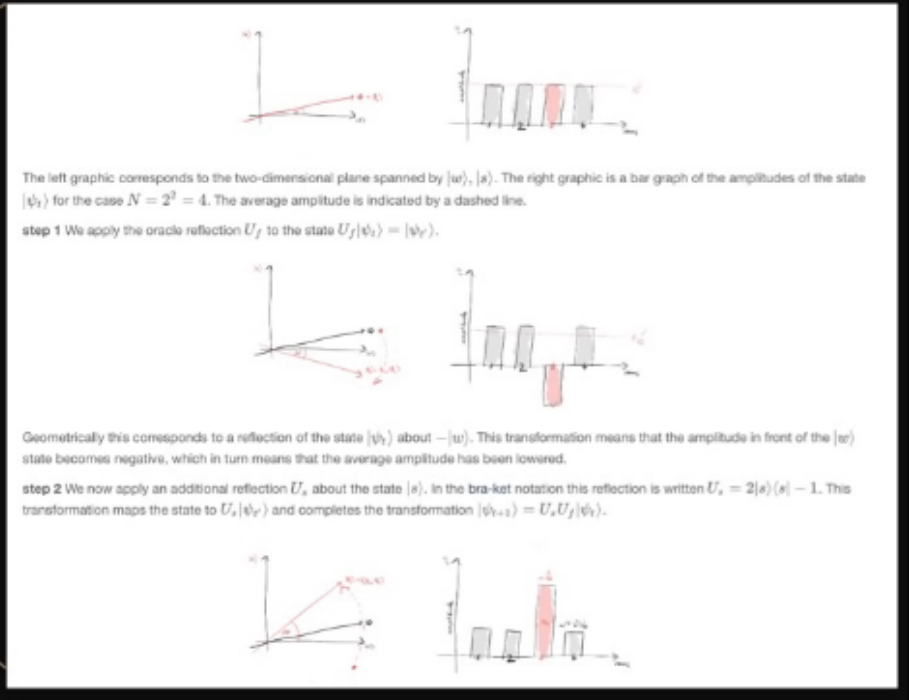
1 2 3 4 5 6 7

Quantum Algorithms

In this section we embark on more complex scores a simply defining entanglement and begin to use it in c future):

- Grover's algorithm
- Deutsch-Jozsa algorithm
- Learning parity with noise
- Phase estimation algorithm
- Shor's Algorithm

1 2 3 4 5 6 7

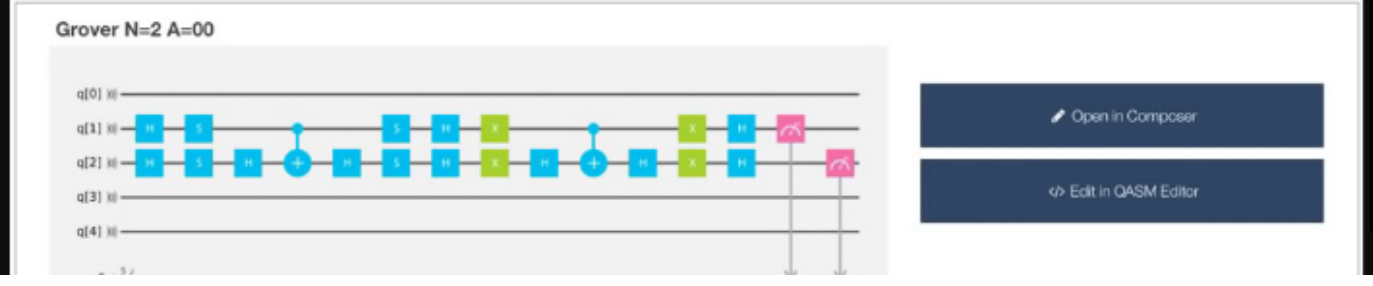


The left graphic corresponds to the two-dimensional plane spanned by $|w\rangle, |s\rangle$. The right graphic is a bar graph of the amplitudes of the state $|\psi_1\rangle$ for the case $N = 2^2 = 4$. The average amplitude is indicated by a dashed line.

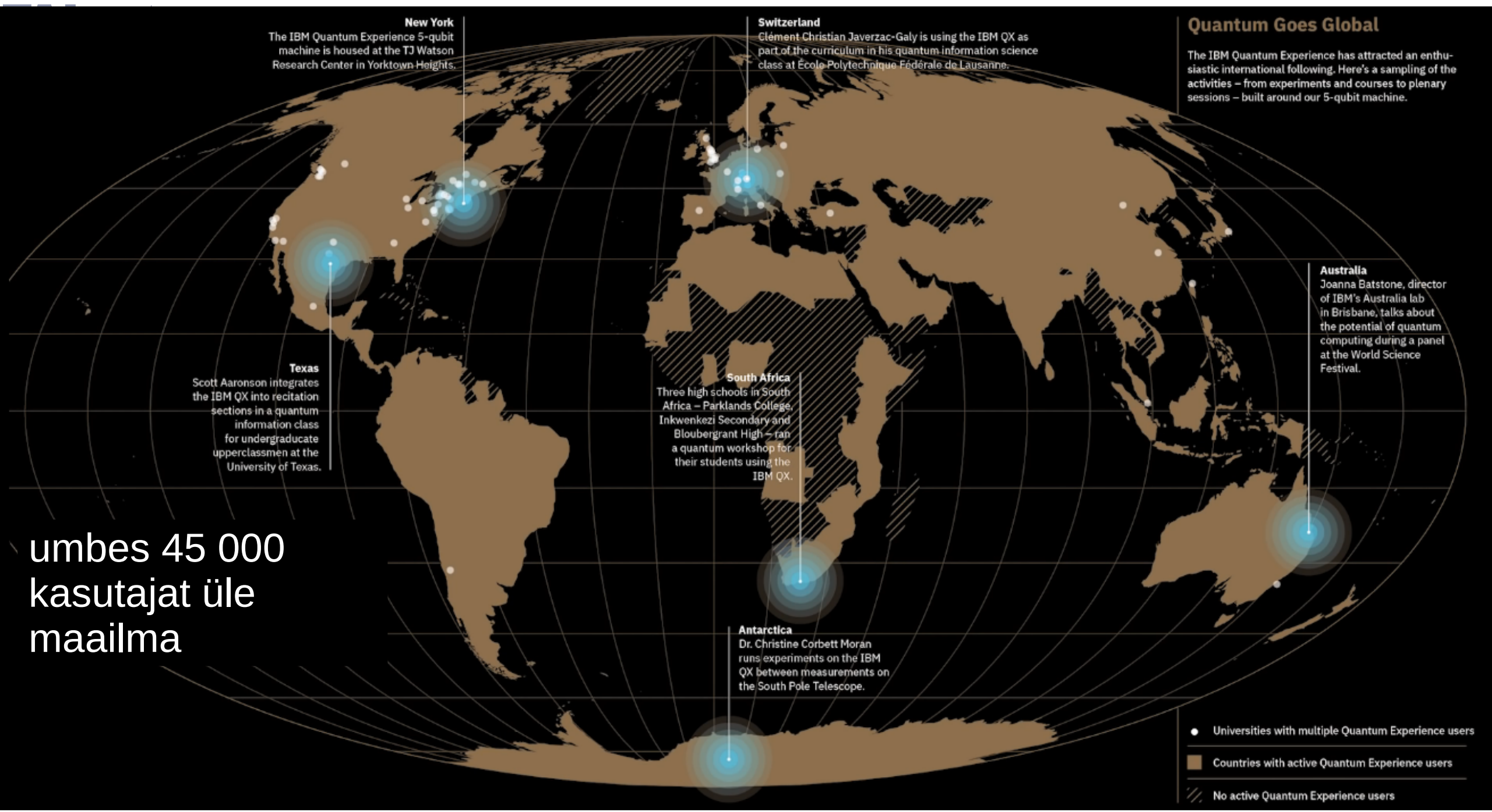
step 1 We apply the oracle reflection U_f to the state $U_f|\psi_1\rangle = |\psi_2\rangle$.

Geometrically this corresponds to a reflection of the state $|\psi_2\rangle$ about $-|w\rangle$. This transformation means that the amplitude in front of the $|w\rangle$ state becomes negative, which in turn means that the average amplitude has been lowered.

step 2 We now apply an additional reflection U_s about the state $|s\rangle$. In the bra-ket notation this reflection is written $U_s = 2|s\rangle\langle s| - 1$. This transformation maps the state to $U_s|\psi_2\rangle$ and completes the transformation $|\psi_{1+1}\rangle = U_s U_f|\psi_1\rangle$.



väravate jada, mis vajalik Grover’i algoritmi jaoks



umbes 45 000 kasutajat üle maailma

Kvantarvutite peal tehakse ka teadust

https://www.youtube.com/watch?v=S52rxZG-zi0

Kvantarvutile tehtud mitmekasutaja mäng

Dr James Wootton Follow

Quantum computation researcher at the University of Basel. Committed to getting the public involve...

Mar 7 · 4 min read

Quantum Battleships: The first multiplayer game for a quantum computer

Like normal Battleships, but simpler and more complex at the same time.

The game is played on IBM's cloud controlled processor. They are real life quantum bits, and you can use them to play a game! They can be little noisy, but that's just the weather buffeting the ship and bombs. Both players will have to learn how best to deal with it.

-- Dr. James Wooton, quantum researcher, U. Basel

```
===== Welcome to Quantum Battleships! =====

  ~~ A game by the Decodoku project ~~


When in doubt, press any key to continue!

This is a game for two players.

Player 1 will choose the position of a Battleship.

Player 2 will try to bomb it.

We start with Player 1.
Look away Player 2!

The lines in the bowtie shape below are the places you can place your ship.

|\     /|
| d   b |
|  \ /  |
f   X   a
|  / \  |
| e   c |
|/     \|

Choose a line for your ship. (a, b, c, d, e or f)

Player 2: You're up!

The numbers below mark places you can bomb.

4       0
|\     /|
| \   / |
|  \ /  |
|   2   |
|  / \  |
| /   \ |
|/     \|
3       1

Choose a position for your first bomb. (0, 1, 2, 3 or 4)
1

Choose a position for your second bomb. (0, 1, 2, 3 or 4)
2

Choose a position for your third and final bomb. (0, 1, 2, 3 or 4)
3
```

Kogukonna ehitamine – kirjutatakse kogemustest, küsitakse küsimusi jne.

Applying a CNOT gate mathematically.

1

I've been teaching myself how to use the composer by doing the quantum computations by hand. I understand the inputs and outputs of a CNOT when considering |0> and |1> controls and targets, but now how to compute the results mathematically. If I could get help on this, I should be able to understand controls and targets in superpositions if I can get the mathematics straight.

gates quantum computing probability cnot General

AN andrewr_ - a day ago

Interpreting results of this circuit?

1

Hello! I've tried to make a Phase Estimation circuit where the unitary U is the pauli-X gate. The PEA is run with 4 bits of precision.

1) Did I implement the circuit properly?

2) When I run the experiment (ideal, single shot) it returns the state |01011>. How do I interpret this result? What does it actually mean? Like does it mean the estimated phase is 0.01011 (in binary)?

PEA for pauli-x

Open in Composer Show Results

General

QU quantumbit - a day ago *(Edited: a day ago)*

What are your best quantum related puns?

2

As our team researches quantum computing, we want to integrate our research into other facets of our lives, such as food and drinks!

What we have so far:

(drinks)
- Gin & tanglement
- Quantopolitan
- Quark & stormy

(food)
- Quntamole

cheers!

quantum puns General

RU russellhuffman - 7 months ago

Hi russellhuffman!

2

Your funny question overcomes one's economical interest. Some ideas (not mine) need to be registered before talking about them. But hard science workers seldom are good for economy and finance, they use to gift their novelties before taking an advantage. This seems an exercise within a brainstorming.

Qushi: quantum sushi, every piece is undistinguishable from each other (perfectly made taste and shape, high reproducibility, thanks to its japanese origin which ensures quality)

Toffoli bone stake: special sort of T-bone stake (highly symmetric once you find the bone)

Pauli potatoes: resembling to noisette potatoes, but having spin symmetry according to Pauli matrices propperties (still under developement, s=1/2)

Clifford salad: this salad is a truly group from an algebraic outlook, since every vegetal can mysteriously be converted into another belonging to the same set (it has got six flavors: charm, strange, top, bottom, up and down).

Bell ring: sweet baked donut-shaped, so tasty that it uses to entangle with a commensal, for dissapearing faster than the speed of light (after an unexpected non-local biological effect, not well understood by our current theories)

Quanturoshka: mix of quantum caipirinha and vodka. Original formulation of quantum caipirinha was fully developed in Brazil by Richard Feynmann (after his famous conference when he called our attention to quantum computing), but its secret is hidden better than Coke's one.

If I find another things to communicate regarding this issue, I will write again. Kind regards!

LE levyug - 7 months ago *(Edited: 7 months ago)*

Reply

https://www.youtube.com/watch?v=S52rxZG-zi0

See on seni üks pikemaid arutlusi kogukonnas – kuidas teha kivi-paber-käärid mängu kvantarvuti peal

4

How to implement Rock Paper Scissors

I understand how to use a Hadamard gate to mimick a coin flip. How can I get a random result from three possiblities (like Rock, Paper, Siccors)? Just looking to get a random selection of 1,2,3.

basics Software

CA **cap10curt** - a month ago

7

@cap10curt

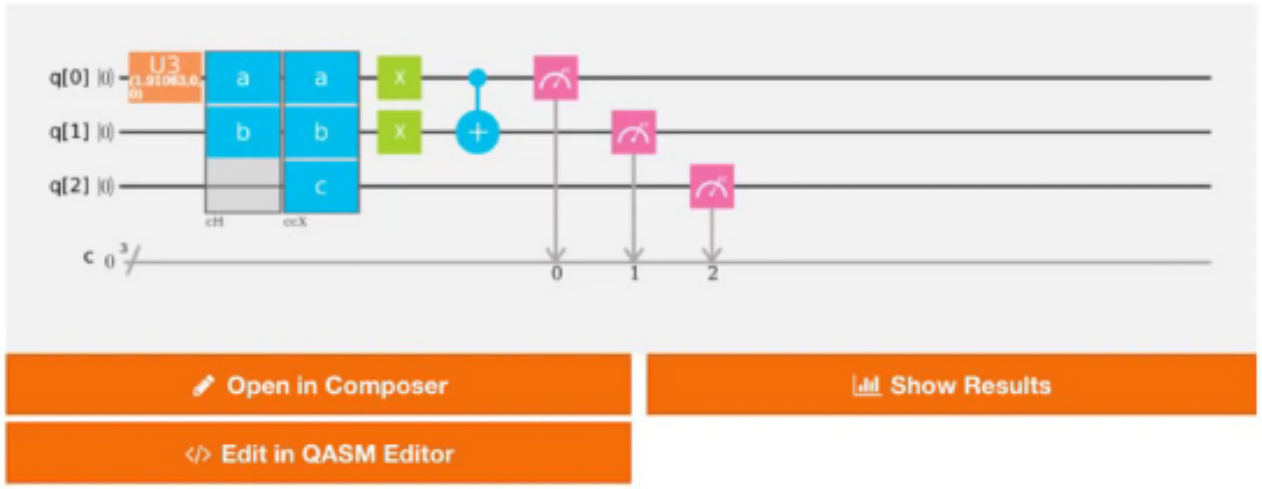
This is an interesting question. One way to do this is to make a W-state, which is the quantum state $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$. This state is hard to make from cnots but here is a circuit that does it (I believe)

The three numbers would then be 1 = 001, 2= 010, and 3 = 100.

Alternatively, you could just use the second case which makes the bits 00, 01, and 11

First the circuit makes a superposition $\sqrt{1/3}|00\rangle + \sqrt{(2/3)}|01\rangle$ then after the cH if the first qubit is in the 1 state it splits the $\sqrt{(2/3)}$ up in two parts making $1/\sqrt{(3)}|00\rangle + \sqrt{(1/3)}|01\rangle + \sqrt{(1/3)}|11\rangle$. The rest of the first circuit just moves the equal superposition around so that it is a W state.

W-state



https://www.youtube.com/watch?v=S52rxZG-zi0

Näide kvantarvuti kasulikkusest

- andmetöötlus
  - tavaarvuti otsib kui inimene raamatust mõnda sõna otsides (mida pole raamatu taga registris-indeksis) – lehitseb lehekülgi, kuni leiab otsitu. Keskeltläbi tuleb otsitava leidmiseks läbi otsida pool raamatut, ehk kui selles on lehekülgi N, siis otsingu aeg on võrdeline suurusega N/2. E-raamatu puhul kulub tänapäevasel tahvelarvutilgi selleks küll vaid sekundeid, kuid kui N kasvab miljonite-triljonite kanti nagu suurandmete puhul, jäävad ka superarvutid selliseks otsinguks liiga aeglaseks.
  - seevastu kvantarvutil jooksval Groveri algoritmil kuluks samaks ülesandeks aega võrdeliselt vaid ruutjuurega N-ist, mis annaks suurte N-ide puhul väga suure ajavõidu

Kvantarvuti Eestis?

- teadaolevalt keegi kvantarvutit Eestis ei ehita
- TÜ füüsikainstituudis uuritakse materjale, mis võivad osutuda perspektiivseiks kvantinfotehnoloogias
- TÜ loeb alates 1998 kvantarvutite ja kvantkrüptograafia aluseid
- kvantfüüsikaga seotud kursused ka TTÜs

Kvantarvuti varsti töölauale?

- kindlasti mitte
- Esiteks, tekstitöötluseks ning tavapäraseks kontoritööks on juba praegustel arvutitel võimsust ja oskusi palju rohkem, kui neid tavaliselt üldse ära kasutatakse.
- Teiseks, praktilist väärtust omav kvantarvuti, kui see luuakse, saab olema vähemalt mitmekümnekilone masinakompleks, roostevabast terasest vaakumkambrite ja -pumpadega ja/või ülimadalaid temperatuure tagavate külmutusseadmete ning muu sellisega.

https://heureka.postimees.ee/3983689/peeter-saari-jargmise-digirevolutsiooni-teeb-kvant-uleolek

Kvantarvuti varsti töölauale?

- Kvantarvuteid hakkaksid pruukima eelkõige riiklikud (sala)kontorid ning suurfirmad – näiteks suurandmete (*big data*) töötlemiseks või uute ravimite kvantkeemiliseks disainimiseks – ja muidugi teaduslaborid.
- Samas on kvantarvuti loomist juba aastaid nähtud 20-aastasel silmapiiril, mis aina edasi nihkub.

https://heureka.postimees.ee/3983689/peeter-saari-jargmise-digirevolutsiooni-teeb-kvant-uleolek

Kvantarvuti loomise peamine põhjus

- erandlik kiirus tänu
  - superpositsioonile (kvantparallelism): 0/1 samaaegselt
  - põimitusele (*entanglement*)
  - 50 kvantbitti kasutava kvantarvuti jõudlus võrreldav umbes 1 000 000 000 000 000 (10^{15} - kvadriljon) transitoriga klassikalise arvutiga

https://novaator.err.ee/683714/kvantarvutite-argikasutusse-joudmist-voib-kiirendada-vana-hea-rani

Kvantarvuti räni baasil

- räni baasil kvantarvutid (2018):
  - kvantbitid jäävad põimituks pikemat aega – saab tehete tegemiseks kasutada pikemat aega
  - võimaldab paremini kalibreerida arvutuste tegemiseks kasutatavaid loogikaväravaid, mille tulemusena saab kvantbitte üksteisele lähemale varasemast tihedamalt ja see tähendab omakorda suuremat arvutusvõimsust
  - tulevikus ehk isegi toat° praeguse ~0K (abs 0) asemel

https://novaator.err.ee/683714/kvantarvutite-argikasutusse-joudmist-voib-kiirendada-vana-hea-rani
https://www.nature.com/articles/nature25766
https://www.nature.com/articles/nature25769

Kvantarvuti ja turvalisus?

- tänane krüpto murtakse?
  - ei kuna tehnoloogia areneb (kvantkrüptograafia)
  - nimetatud kaks kvantfüüsika veidrust (superpositsioon, põimumine) võimaldavad luua pealtkuulamiskindlaid sideliine (on ka juba teostatud)
  - aprillis 2004 tehti sellise salaside abil rahaülekanne kahe panga vahel optilise kaabli vahendusel

https://novaator.err.ee/258533/teadlane-sonumisaladust-aitab-kaitsta-kvantkruptograafia
https://www.fyysika.ee/?p=4003
https://www.youtube.com/watch?v=6H_9l9N3IXU

Kvantarvuti ja turvalisus?

- Riigi Infosüsteemi Ameti kodulehel ilmuvad regulaarselt ülevaated
  - Küberturvalisus -> RIA uuringud, analüüsid, ülevaated
  - 2018: Postkvantkrüptograafia ülevaade
  - 2017: Krüptograafiliste algoritmide elutsükli uuring

https://www.ria.ee/et/ametist/uuringud-analuusid-ulevaated.html

Kvantarvuti ja turvalisus?

Aggarwal jt. ennustasid aastal 2017, et ühes arvutis kasutada olevate kvantbittide arv jõuab 10000-ni ajavahemikus 2025–2035. Kuna nende hinnangud tuginevad vaid väga piiratud arvule andmepunktidele, tuleb sellesse ennustusse suhtuda üsna kriitiliselt.

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 8

Kvantarvuti ja turvalisus?

- Kui realiseerub kõige optimistlikum kvantarvuti valmimise stsenaarium, jääb järgmise ID-kaardi põlvkonna eluiga sellesse perioodi juba osaliselt sisse.
- Seetõttu tuleks uues ID-kaardi (või üldisemalt igas eID platvormi) hankes juba arvestada vajadusega võtta kasutusele kvantarvutikindlaid algoritme.

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 8

Kvantarvuti ja turvalisus?

- Krüptograafiliste algoritmide soovitatavad võtmepikkused
  - veerg “DSA, DH” viitab DSA signatuurialgoritmile ja Diffie-Hellmani võtmevahetusele üle jäägiklassiringi, kus avaliku ja salajase võtme soovitatavad pikkused on vastavalt L ja N
  - veerg “RSA” annab soovituse RSA algoritmi mooduli pikkusele
  - veerg “ECC” aga elliptkõveratele tuginevate krüptoalgoritmide võtmepikkustele
  - veerud “Plokkšifrid” ja “SHA-2, SHA-3” soovitavad vastavalt sümmeetriliste algoritmide võtmepikkust ning räsifunktsioonide väljundi pikkust
  - peamiseks soovitatavaks sümmeetriliseks krüptoalgoritmiks on jätkuvalt AES

Turvatase	DSA, DH	RSA	ECC	Plokkšifrid	SHA-2, SHA-3
128	$L = 3072, N = 256$	3072	256 . . . 383	128	256
192	$L = 7680, N = 384$	7680	384 . . . 511	192	384
256	$L = 15360, N = 512$	15360	512+	256	512

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 9

Kvantarvuti ja turvalisus?

- USA agentuur NSA (*National Security Agency*) ei soovita kvantarvutite peatse ilmumise kartuses uutes rakendustes kasutada elliptkõveraid lühema kui 384-bitise võtmega ega AES-i lühema kui 256-bitise võtmega.
- See soovitus oli ka üheks põhjuseks, miks Eesti ID-kaardi uute krüptoalgoritmide aluseks valiti elliptkõver P-384

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 9

Kvantarvuti ja turvalisus?

Üldotstarbelisel kvantarvutil saab Groveri algoritmi abil kiirendada sümmeetriliste šifrite (näiteks AES *Advanced Encryption Standard*) *k*-bitise võtmeruumi täielikku läbivaatust 2^k sammult $2^{k/2}$ sammuni. Selleks vajalike kvantbittide arv on toodud allolevas tabelis

AESi võtmepikkus	**Vajalike kvantbittide arv**
128	2953
192	4449
256	6681

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 8
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Kvantarvuti ja turvalisus?

- Proos ja Zalka leidsid, et n-bitise RSA mooduli tegurdamiseks on vaja umbes 2^n kvantbitti ning n-bitises elliptkõverarühmas diskreetse logaritmi leidmiseks on vaja umbes 6^n kvantbitti
- Seega näiteks on 2048 -bitise RSA murdmiseks vaja umbes 4096 ning kõveral P-256 diskreetse logaritmi arvutamiseks umbes 1500 kvantbitti.
- Proos ja Zalka märgivad ka, et füüsiliste kvantbittide ebastabiilsuse tõttu tuleb Shori algoritmis kasutatavatele bittidele lisada veaparandusliiasust, mistõttu praktikas võivad need arvud olla paar korda suuremad.

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 7

Kvantarvutid võrku?

- (2018) Üks töörühm toimetas Šveitsis ETH Zürichis, seda juhtis Andreas Wallraff ja sellesse kuulus ka eestlasest doktorant Johannes Heinsoo; teine rühm talitas Hollandis Delfti Tehnikaülikoolis Peter Humphreysi eestvedamisel.

https://novaator.err.ee/839640/tookindel-poiming-uhendab-kvantarvutid-vorku

Kvantarvutid võrku?

- Zürichis tehtud katses kinnitasid teadlased kahe kvantprotsessori vahele meetri pikkuse kaabli. Mõlema protsessori sees oli kvantbitt, mis teatava signaali peale kiirgas välja üksiku footoni, mis kandis kvantbitis salvestatud kvantinformatsiooni, liikus koos selle infoga läbi kaabli teises protsessoris asunud kvantbitini ja neeldus seal, andes info üle ja viies sellega kaks kvantbitti omavahel kvantpõimingusse.

https://novaator.err.ee/839640/tookindel-poiming-uhendab-kvantarvutid-vorku

Kvantarvutid võrku?

- Samalaadseid katseid on tehtud ka varem, aga seni ei ole teadlastel olnud kontrolli selle üle, millal täpselt footon suvatseb kvantbitist välja kiirguda ja mis kuju tal seejuures on. Vale kujuga footon ei tarvitse piisavalt hästi neelduda. Nüüd aga läks korda nii footoni kiirgushetk kui ka kuju kontrolli alla saada ja sellest läks side kahe protsessori vahel hulga tõhusamaks.

https://novaator.err.ee/839640/tookindel-poiming-uhendab-kvantarvutid-vorku

Kvantarvutid võrku?

- Hollandis tehtud katses aga mindi natuke teist teed. Seal ei mindud ühe korraga kindla peale põimingut looma, vaid tehti lühikese ajaga palju kordi proovi, püüdes seejuures edutõenäosust võimalikult kõrgeks ajada. Nii õnnestuski saavutada olukord, kus kahe kvantbiti vahel tekkis põiming keskmiselt kümme korda kiiremini kui katkes, nii et kokkuvõttes sai side päris püsiv.

https://novaator.err.ee/839640/tookindel-poiming-uhendab-kvantarvutid-vorku

Kvantinternet?

- Hiina teadlastel õnnestus (2017) juba paar kuud pärast esimese kvantsidesatelliidi orbiidile saatmist põimida omavahel enam kui 1200 kilomeetri kaugusel asuvad valgusosakesed. Saavutus sillutab teeb üliturvalistele sidesüsteemideni ja toob lähemale tõelise kvantinterneti.

https://novaator.err.ee/602511/hiinlaste-saavutus-toob-lahemale-uliturvalise-kvantinterneti

Kvantinternet?

- Üliturvaline andmeside põhineb omavahel põimitud pisiosakestel nagu footonitel. Kvantmehaanika seaduspärade alusel saavad need üksteist mõjutada paiknedes isegi universumi erinevatest otstes. Mõõtes ühe valgusosakese omadusi on koheselt teada ka teise omadused nagu valguslaine võnkesuund ehk polarisatsioonid. Näiteks jagavad taoliselt omadusi samaaegselt loodud footonid.

https://novaator.err.ee/602511/hiinlaste-saavutus-toob-lahemale-uliturvalise-kvantinterneti

Kvantinternet?

- Sarnaselt tavapärastele valguskaablites liikuvatele osakestele saab ka neid kasutada andmete krüpteerimiseks kasutatud võtmete vahetamiseks. Erinevalt tavalistest footonitest on aga põimituse tõttu teada, kui keegi teele saadetud valgusosakese vahepeal kinni püüab ja mõõdab andmetele ligipääsemiseks näiteks selle polarisatsiooni. Omavahel suhelnud inimesed saavad seeläbi võtme kasutamise lõpetada ja vahetada ebaturvalise kanali turvalisema vastu.

https://novaator.err.ee/602511/hiinlaste-saavutus-toob-lahemale-uliturvalise-kvantinterneti
https://novaator.err.ee/851770/kogu-maailma-internetiliiklus-mahuks-uhte-vorgukaablisse

Kvantarvutite ajalugu lühidalt

- 1960-ndatel paneb Stephen Wiesner aluse krüptograafilisele töövahendile, mis saab aluseks kvantprogrammeerimisele
- 1970-ndatel arenesid erinevad teooriad: Holevo teoreem, kvantinfo teooria jt
- 1980-ndatel abstraktsed kvantarvuti mudelid
- 1990-ndatel arenevad erinevad kvantalgoritmid (sh veaparandus), esimene kvantloogikavärav, 2- ja 3-kvantbitine NMR (*Nuclear Magnetic Resonance*) kvantarvuti, esmakordne Groveri algoritmi kasutamine, põimumist kasutav turvaline side

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
https://en.wikipedia.org/wiki/Quantum_programming
https://en.wikipedia.org/wiki/Quantum_information_science
https://en.wikipedia.org/wiki/Grover's_algorithm

Kvantarvutite ajalugu lühidalt

- 2000-ndatel 5-, 7-, 12-kvantbitine kvantarvuti, mitmed kvantolekute põimumise katsed, mitmed uued lähenemised ja läbimurded (kvantoleku vahetamine valguse ja mateeria vahel, kvanttransistori mudel jne), rohkelt avastusi ja arenguid, 28-kvantbitine QA (*Quantum Annealing*) kvantarvuti, väidetavalt 128-bitine kvantkiip (kinnitamata andmeil)
- 2010-ndatel tehnoloogilised arengud (uus jahutussüsteem, ühe-elektroni kvantbitt, kvantantenn jne), 84-, 1000-, 2000-kvantbitine kvantarvuti (D-Wave Systems), IBM: 20-,50-kvantbitine kvantarvuti, 300-kvantbitine simulaator, teemantil põhineva arhitektuuri avaldamine, info kvantteleportatsioon 0% veateguriga ~3m kaugusele – püüdlus kvantinterneti poole; 2018 lõpus USA president Trump allkirjastab National Quantum Iniative Act – 10a plaan kiirendamaks kvantarvutite ja sellega seonduva arengut USAs

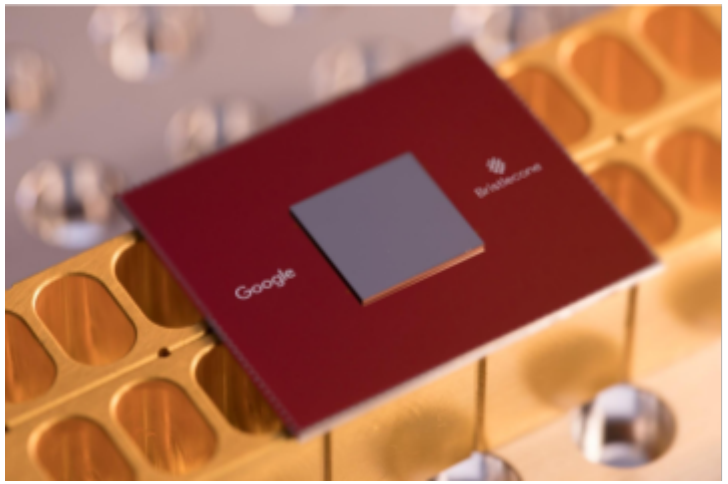
https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
https://en.wikipedia.org/wiki/Quantum_annealing

D-Wave 2000Q (2017)

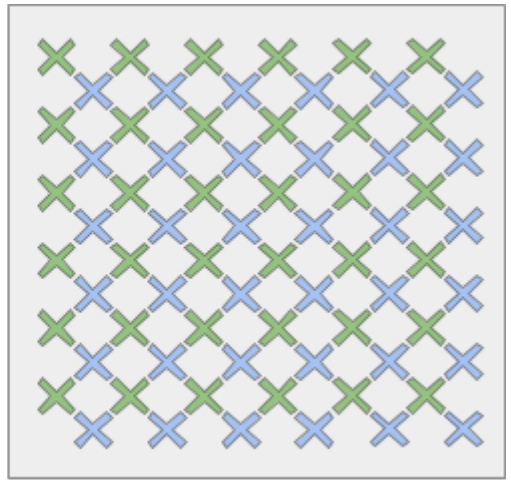
- ettevõte D-Wave Systems
- nimi: D-Wave 2000Q
- pressiteade 24.01.2017
- 2000 kvantbitti
- *Quantum Annealing* baasil
- QPU (kvantprotsessor)
  - -273°C
  - kõrge vaakum: 10 mrd kord väiksem Maa atmosfäärirõhust
  - energiakulu 25 kW (üle 10x vähem kui tavalised superarvutid)
- lisainfo (PDF)

Google: Bristlecone (2018)

- Google AI labor, 2018
- nimi: Bristlecone
- 72 kvantbitti
- loogikaväravate baasil
- ülijuhtidel põhinev



Bristlecone'i kvantprotsessor

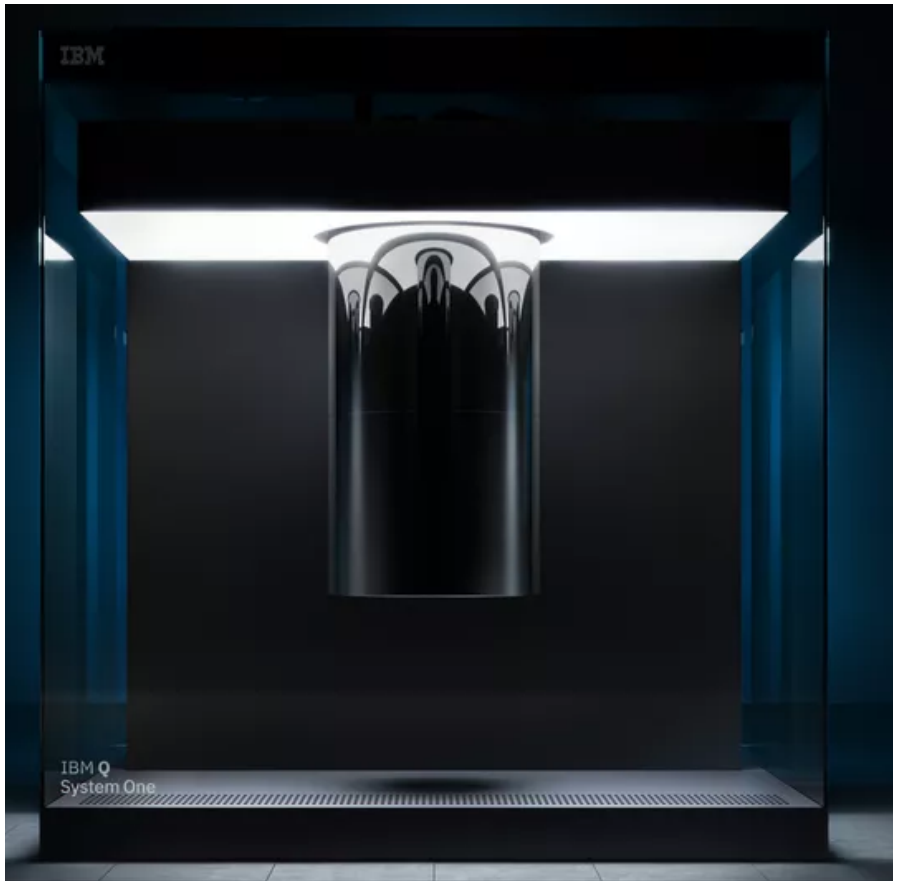


Protsessori joonis: iga ristike kujutab kvantbitti ühenduses lähima naabriga

https://novaator.err.ee/687992/google-asus-testima-suurimat-kvantarvutit
https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
https://research.google.com/pubs/QuantumAI.html -> https://ai.google/research/pubs?area=QuantumAI

IBM: Q System One (2019)

- nimi: Q System One
- 20 kvantbitti
- loogikaväravate baasil
- püsivara (*firmware*) võimaldab uuendada süsteemi tööd katkestamata
- veebis kasutatav nov 2017 alates



https://www.theverge.com/2019/1/8/18171732/ibm-quantum-computer-20-qubit-q-system-one-ces-2019
https://www.research.ibm.com/ibm-q/system-one/ , https://www.youtube.com/watch?v=LAA0-vjTaNY intro
https://ibm.com/quantumcomputing , https://www.youtube.com/watch?v=y0AjmgMSftA building Q (high speed)
https://www.youtube.com/watch?v=wfsUxdYSOFs - miks vajame & kuidas kasutada Q'd

Kvantprotsessorite arengud

Gate model (universal) quantum processors [edit]

Further information: Quantum circuit and Quantum logic gate

These QPUs are based on the quantum circuit and quantum logic gate-based model of computing.

Manufacturer	Name/Codename/Designation	Architecture	Layout	Socket	Fidelity	Qubits	Release date
Google	N/A	Superconducting	N/A	N/A	99.5% [1]	20 qb	2017
Google	N/A	Superconducting	7×7 lattice	N/A	99.7% [1]	49 qb [2]	Q4 2017 (planned)
Google	Bristlecone	Superconducting	6×12 lattice	N/A	99% (readout) 99.9% (1 qubit) 99.4% (2 qubits)	72 qb [3][4]	5 March 2018
IBM	IBM Q Experience 5	Superconducting	N/A	N/A	N/A	5 qb	2016 [1]
IBM	IBM Q Experience 16	Superconducting	2×8 lattice	N/A	N/A	16 qb [5]	17 May 2017
IBM	IBM Q 17	Superconducting	N/A	N/A	N/A	17 qb [5]	17 May 2017
IBM	IBM Q 20	Superconducting	N/A	N/A	N/A	20 qb [6]	10 November 2017
IBM	IBM Q 50 prototype	Superconducting	N/A	N/A	N/A	50 qb[6]	
Intel	17-Qubit Superconducting Test Chip	Superconducting	N/A	40-pin cross gap	N/A	17 qb [7][8]	10 October 2017
Intel	Tangle Lake	Superconducting	N/A	108-pin cross gap	N/A	49 qb [9]	9 January 2018
Rigetti	19Q	Superconducting	N/A	N/A	N/A	19 qb [10]	December 2017

https://en.wikipedia.org/wiki/List_of_quantum_processors

Kvantprotsessorite arengud

Annealing quantum processors [edit]

Further information: Quantum annealing

These QPUs are based on quantum annealing.

Manufacturer	Name/Codename/Designation	Architecture	Layout	Socket	Fidelity	Qubits	Release date
D-Wave	D-Wave One (Ranier)	Superconducting	N/A	N/A	N/A	128 qb	11 May 2011
D-Wave	D-Wave Two	Superconducting	N/A	N/A	N/A	512 qb	2013
D-Wave	D-Wave 2X	Superconducting	N/A	N/A	N/A	1152 qb	2015
D-Wave	D-Wave 2000Q	Superconducting	N/A	N/A	N/A	2048 qb	2017
Note: Quantum annealers are intended for use in specific technical applications.							

Quantum Annealing (QA) – kvantlõõmutamine (kuumutamine+aeglaselt jahutamine) on metaheuristiline meetod konkreetse objektiivfunktsiooni globaalse miinimumi leidmiseks antud kandidaatlahenduste kogumi (kandidaatolekud) kaudu, kasutades kvantkõikumisi.
Heuristika on loogikavõtete ja metoodiliste juhiste kogum; neid käsitlev teadusharu.
QA kasutatakse mittepidevate (diskreetsete) probleemide lahendamiseks – mitmemõõtmeliste funktsioonide uus minimeerimise meetod.

https://en.wikipedia.org/wiki/List_of_quantum_processors

2018.a arengud

- uus riistvara ja veebipõhised ressursid
- kasvav ärihuvi
- arutelu kvantüleoleku teemadel (*quantum supremacy*)

https://www.youtube.com/watch?v=CeuIop_j2bI

2018.a arengud

- kvantarvutite riistvara arendajad
  - IBM
  - Alibaba
  - Microsoft
  - Google
  - Intel
  - D-Wave Systems
  - Quantum Circuits
  - IonQ
  - Rigetti
  - jt

https://www.youtube.com/watch?v=CeuIop_j2bI
https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication

2018.a kvantarvutite arengud

- IBM pakub tasuta veebis kvantarvuti kasutamist alates nov 2017
- IBM'ilt vabavaraline raamistik Qiskit (nov 2017 alates)
- IBM pakub ka pilvepõhist ligipääsu kvantarvutitele https://www.research.ibm.com/ibm-q/technology/devices/
- Alibaba pakub 11 kvantbitist kvantarvutit
- ka Microsoft pakub kvantarvutit, sh nov 2017 alates arenduskomplekti Q#

https://www.youtube.com/watch?v=CeuIop_j2bI , https://qiskit.org

2018.a kvantarvutite arengud

- 2018 märtsis tuleb Google välja 72 kvantbitise Bristlecone’iga
- novembris 2017 tuleb Intel välja 17 kvantbitise QuTech’iga
- jaanuar 2018 teatab Intel 49 kvantbitise protsessori Tangle Lake valmimisest
- juuni 2018 teatab Intel 26 kvantbitise „pöörlevate kvantbittidega” protsessori valmimisest

2018.a kvantarvutite arengud

- rakendused
  - molekulide jt materjalide modelleerimine
  - lennusimulatsioonid (Lockheed Martin)
  - akude simulatsioon elektriautode arendamiseks (Daimler)
  - logistika optimeerimine (nt Daimler), liikluse optimeerimine (Volkswagen)
  - finantsmodelleerimine (JPMorgan, Barclays)
  - ravimite, narkootikumide avastamine (Accenture Labs, Biogen, 1Qbit)
  - krüptograafia
  - tehisintelligents

2018.a kvantarvutite arengud

- mitte kõik kvantbitid ei ole võrdsed (nt D-Wave vs teised tehnoloogiad)
- kuigi D-Wave on ehitanud 2000 kvantbitise masina siis ei tähenda, et see võimsam oleks kui teistel firmadel
- veaparandus: meil võib vaja olla 10 000+ kvantbitti, et luua veakindlad 100+
- IBM ennustab 5a, Intel 10a kui kvantarvuti tuleb massidesse

Tulevik?

- kõige olulisemaks tundmatuks suuruseks võtmepikkuste eluea hindamisel on üldotstarbeliste kvantarvutite arenduskiirus
- 2017. aasta oktoobris teatas Intel 17-bitise ülijuhtiva kvantkiibi väljalaskmisest
- Google'i teadurid on hinnanud, et tänaste klassikaliste arvutite jõudluse ületamiseks mõnes funktsioonis piisab kvantarvutist, kus on umbkaudu 50 ülijuhtivusel põhinevat kvantbitti

https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf lk 7
https://newsroom.intel.com/news/intel-delivers-17-qubit-superconducting-chip-advanced-packaging

Viiteid

- http://www.nature.com/news/quantum-computers-ready-to-leap-out-of-the-lab-in-2017-1.21239 (2017)
- http://www.nature.com/news/google-moves-closer-to-a-universal-quantum-computer-1.20032 (2016)
- http://www.idquantique.com/quantum-safe-crypto/
- https://novaator.err.ee/260223/fuusikud-esitlesid-suuremootmelise-kvantarvuti-kavandit (2017)
- https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/
- arengud
  - https://www.youtube.com/watch?v=CeuIop_j2bI - 2018.a kvantarvutite arengud
  - https://www.youtube.com/watch?v=iYESkqXVWa0 - 2017.a kvantarvutite arengud
  - https://www.explainingcomputers.com/quantum.html
- https://quantumcomputingreport.com
- mängud
  - https://novaator.err.ee/258861/arvutimang-muudab-kvantmaailma-eksperdiks-ka-paadunud-humanitaari
  - https://www.scienceathome.org

Viiteid

- võimalus testida kvantarvutit, arendusvahendid
  - https://www.dwavesys.com/take-leap (D-Wave)
  - https://quantumexperience.ng.bluemix.net/ (IBM) – Jupyter Notebooks written in Python
  - http://quantumcomputer.ac.cn/ (Alibaba)
  - https://www.microsoft.com/quantum/ (Microsoft)
    - https://www.microsoft.com/quantum/development-kit - Microsoft Q#
  - http://rigetti.com/forest - Rigetti pakutav Forest SDK, python kvantarvutitel
- tutvustused
  - https://www.youtube.com/watch?v=S52rxZG-zi0 (IBM intro to quantum computing)
  - https://www.youtube.com/watch?v=OWJCfOvochA (IBM intro, different levels of understanding)
  - https://www.youtube.com/watch?v=KZf4BSmgdO4 - IBM intro to Q Lab

Viited

- https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
- https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication
- https://en.wikipedia.org/wiki/List_of_quantum_processors
- https://en.wikipedia.org/wiki/Category:Quantum_information_scientists

TALLINNA TEHNIKAÜLIKOOL
IT KOLLEDŽ

Edmund Laugasson
Raja 4C, kab 516, 12616 Tallinn,
Tel +372 628 5842, edmund.laugasson@itcollege.ee
itcollege.ee