

Kvantumszámítógépek programozása

Asbóth János^{1,2}

1: BME TTK Elméleti Fizika Tanszék;

2: Wigner Fizikai Kutatóközpont,
Kvantumoptikai és Kvantuminformatikai Osztály

asboth.janos@ttk.bme.hu

A mai előadás

Mi a kvantumszámítógép?

“kvantumos furcsaságokat” - szuperpozíció, összefonódás
számítási célokra felhasználó gép

Mire jó?

Néhány nehéz feladatra jobb, mint a mai számítógépek

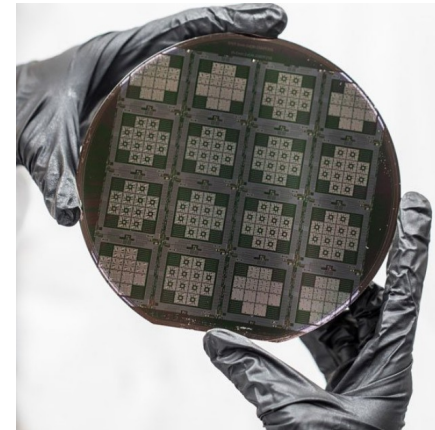
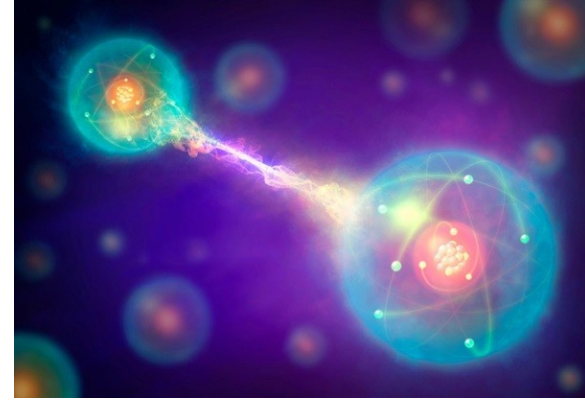
- Molekuláris reakciók szimulálása
(új gyógyszerek, jobb műtrágya)
- Titkosítás feltörése (RSA)
- ??

Mikor lesz?

Nagyon korai fázisú kutatás-fejlesztés

- Többféle hardver
- legjobb gép 53 bites (~1 millió bit kéne)
- IBM gépe online elérhető, kipróbálható

Magyarországon is kutatunk-fejlesztünk
kvantumtechnológiát

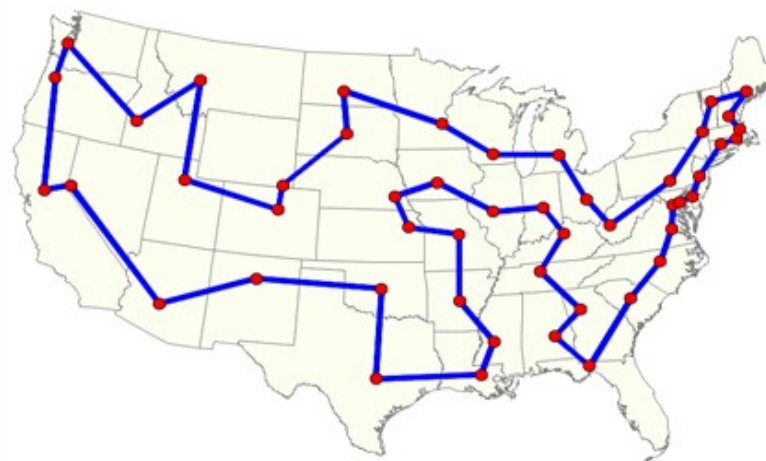


Vannak (exponenciálisan) nehéz feladatok, amiken csak picit segít a gyorsabb számítógép

Utazó ügynök probléma: melyik a legrövidebb út, ami minden várost érint?

2x sebesség → +1 város

(a legjobb egzakt algoritmusnak, de 1%-os hibájú közelítések hatékonyak, ld. wikipedia)



Prímtényezőkre bontás: milyen prímszámokból áll össze a nagy szám?

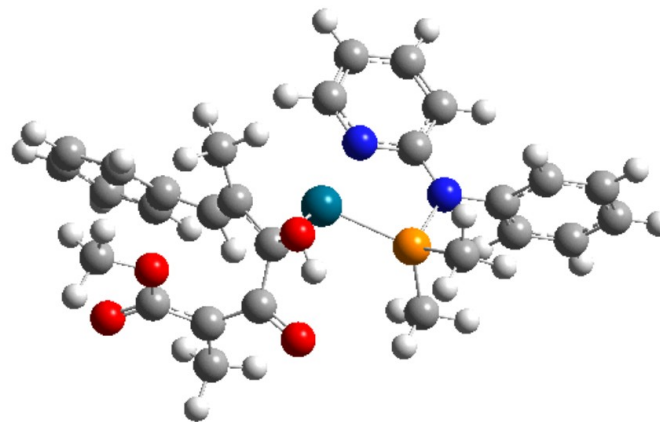
$$502\ 560\ 280\ 658\ 509 = 15\ 485\ 863 * 32\ 452\ 843$$

2x sebesség → +néhány számjegy

(szubexponenciális skálázás, általános számtest-szita
(GNFS) algoritmus)

Kémiai reakciók pontos modellezése

2x memória → +1 elektronpálya



A kémiai reakciók pontos számolása a kvantumos furcsaságok miatt nehéz: szuperpozíció, összefonódás



Bohr 1913

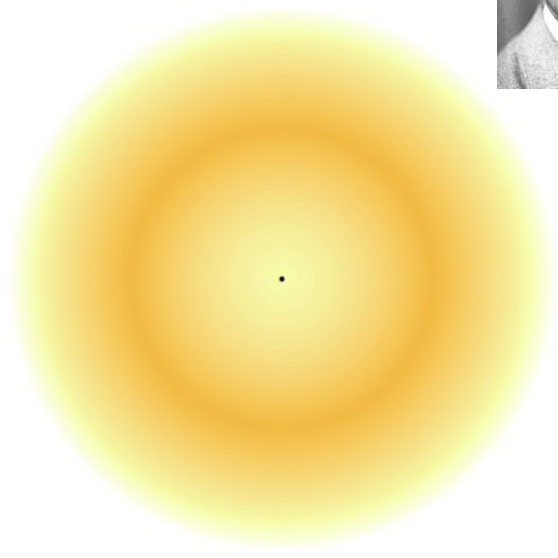
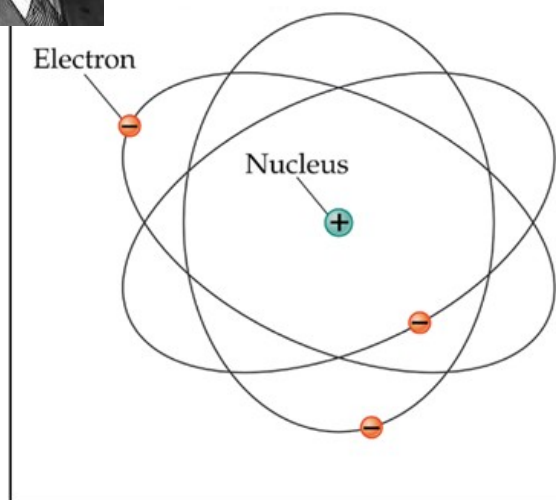


Schrödinger 1925



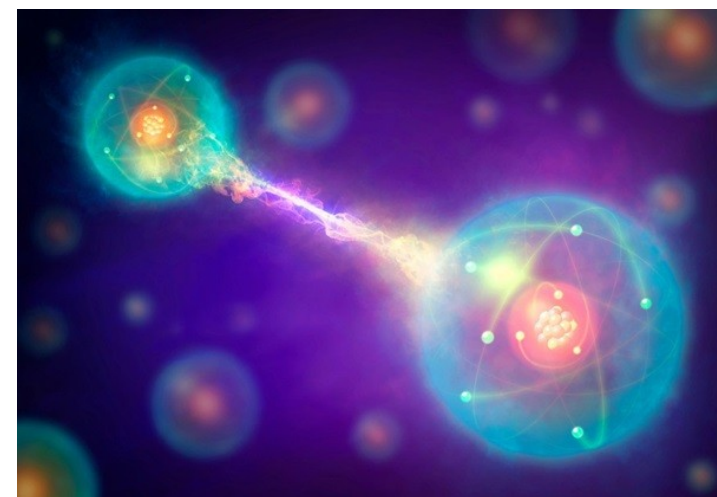
What An Electron Isn't

What An Electron Is



elektron “egyszerre több helyen” lehet
– szuperpozíció.

Csak így tudunk számot adni a
kísérletekről

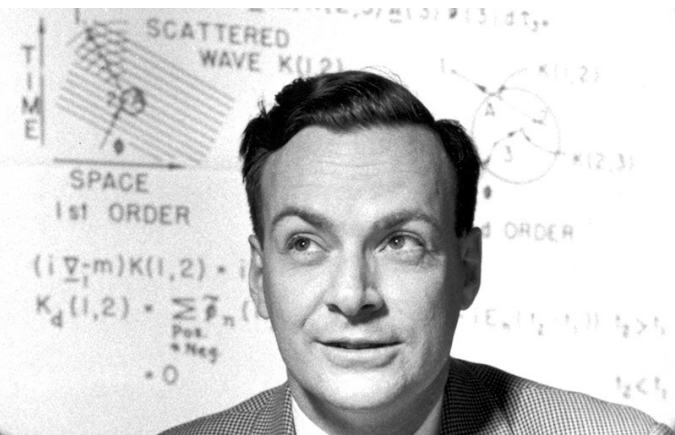


Több elektron
→ egymástól függő szuperpozíciók
= összefonódás

exponenciálisan bonyolult,
de néha ettől hatékony
kémiai reakció

1935- Paradoxonok ellenére a kvantummechanika a modern tudomány és technológia alapja

R. Feynman: Kvantum-elektrodinamika,
1965



SHUT UP
AND
CALCULATE

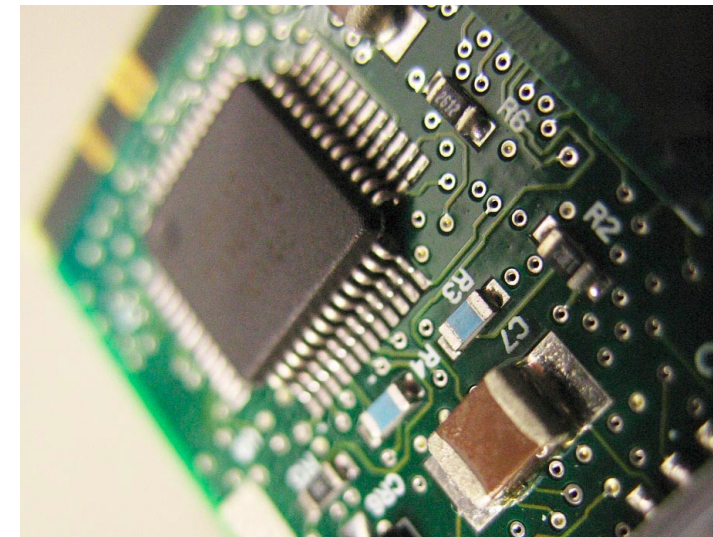


J. Bardeen

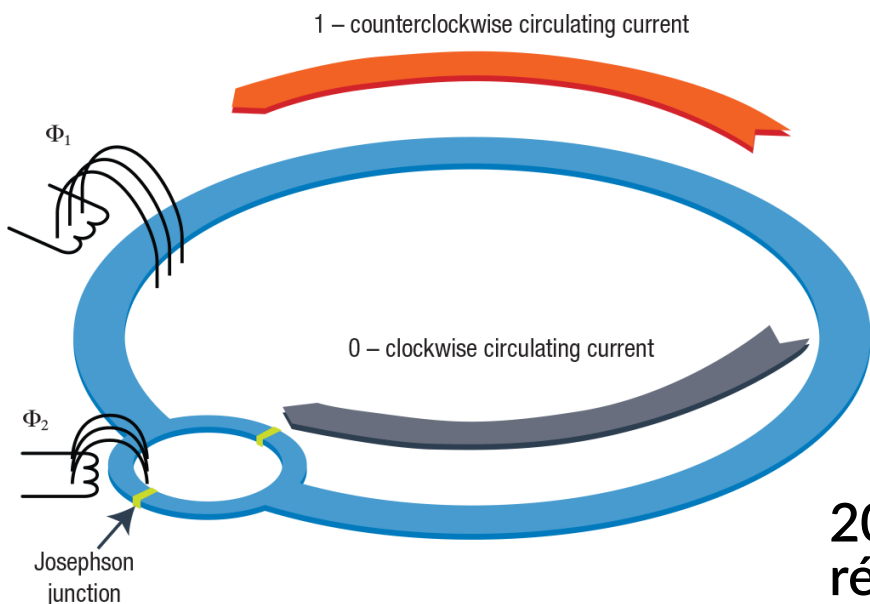
Tranzisztor
1956



Szupravezetés
elmélete
1972



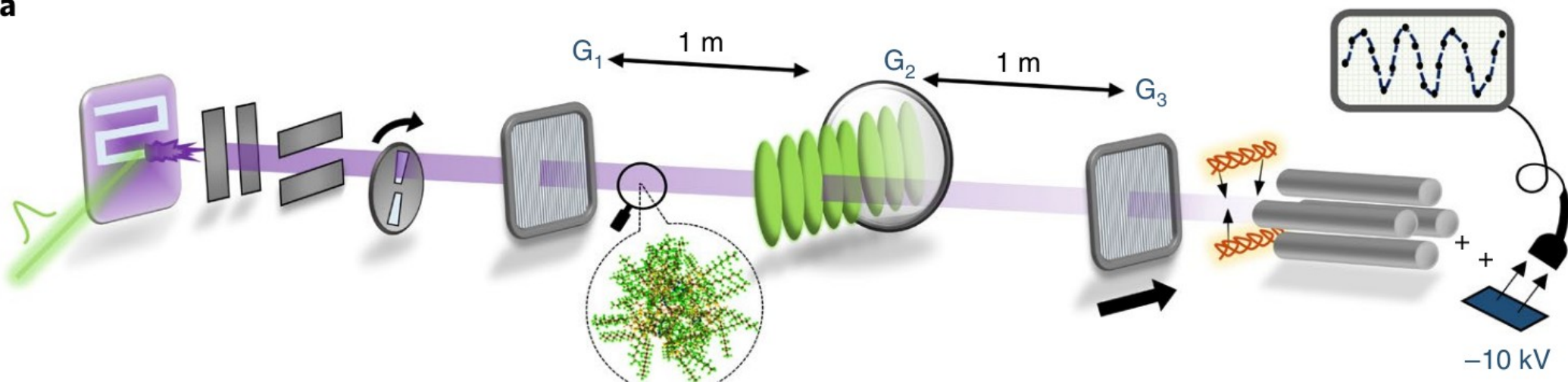
Az 1990-es évek óta a “kvantumparadoxonokat” közvetlenül, kísérletben vizsgálhatjuk



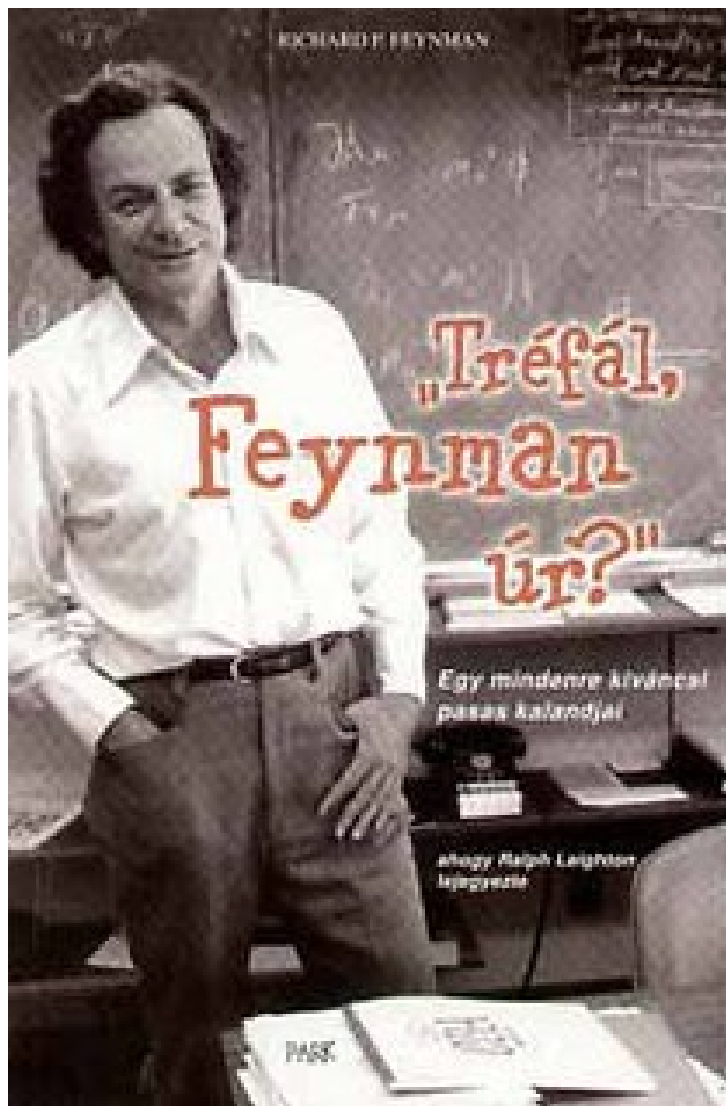
Szupravezető gyűrűben áram jobbra és balra megy körbe “egyszerre” [Mooij, Delft, 2001]

2000 atomos óriásmolekulák is egyszerre két résen tudnak átmenni [Arndt, Bécs, 2019]

a



Feynman, 1981: Ha egyszer a kvantumkémiai számolások ilyen nehezek, kéne ezekhez egy “kvantum-számítógép”



.. trying to find a computer simulation of physics seems to me to be an excellent program to follow out. . . . the real use of it would be with quantum mechanics. . . .

if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

Kvantumszimulátor vagy digitális számítógép?

Ha digitális, mik a kvantumbitek?

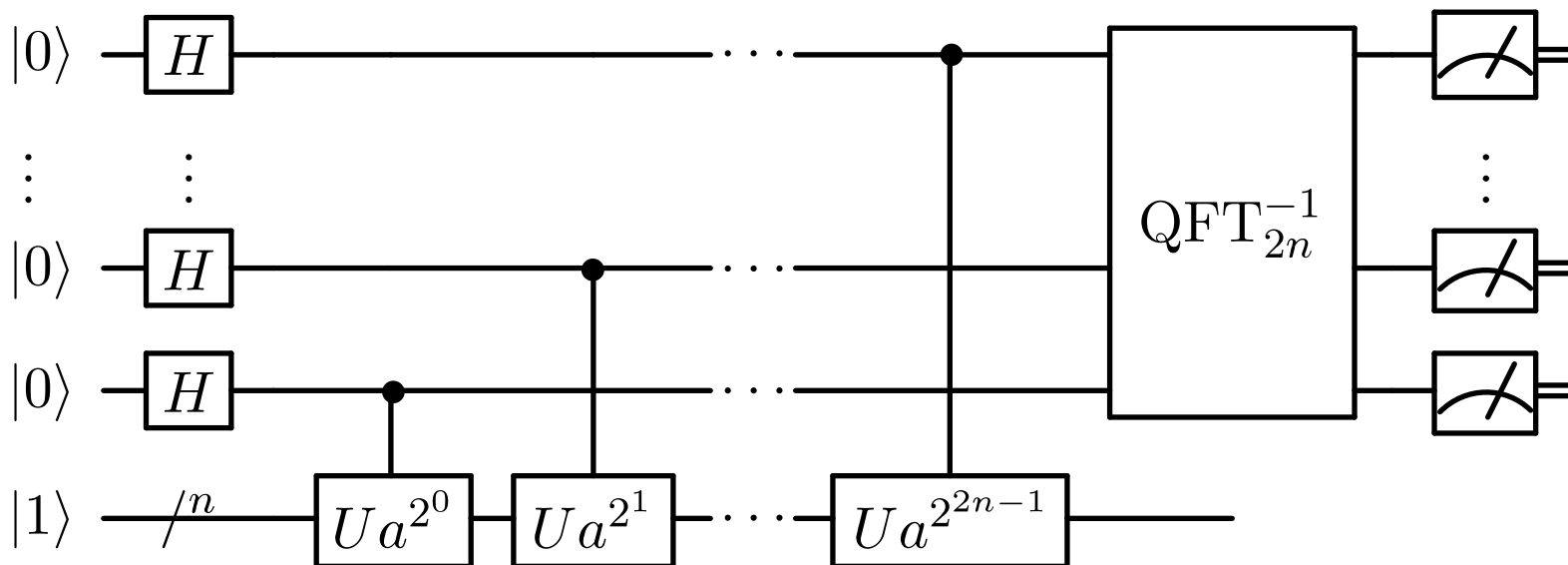
Hogy nézne ki egy program?

Miből lenne a számítógép?

1994, Peter Shor (MIT): Ha lenne kvantumszámítógép, gyorsan tudna prímtényezőkre bontani

Peter Shor, MIT (1959-)

- 1994: prímtényezőket találó kvantum algoritmus
 - exponenciálisan gyorsabb!
- 1996: kvantum hibajavítás

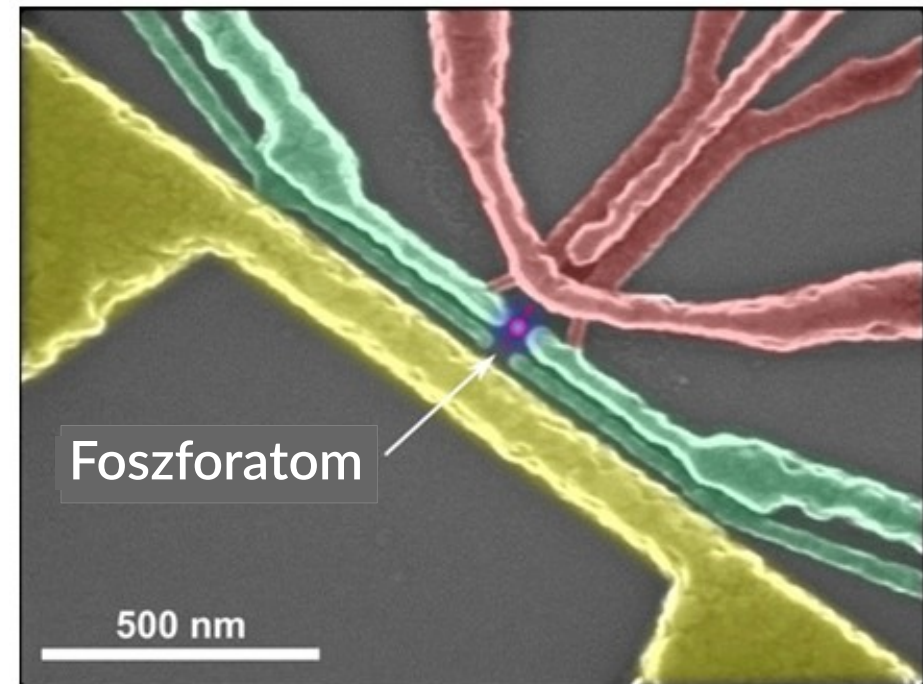


A kvantumszámítógéphez kellenek kvantumbitek.
Ezek a környezettől jól elszigetelt, egyedi
kvantumrendszerek, amiken műveleteket tudunk végezni.

Chris Monroe, USA,
Joint Quantum Inst.:
vákuumban lebegtetett ionok



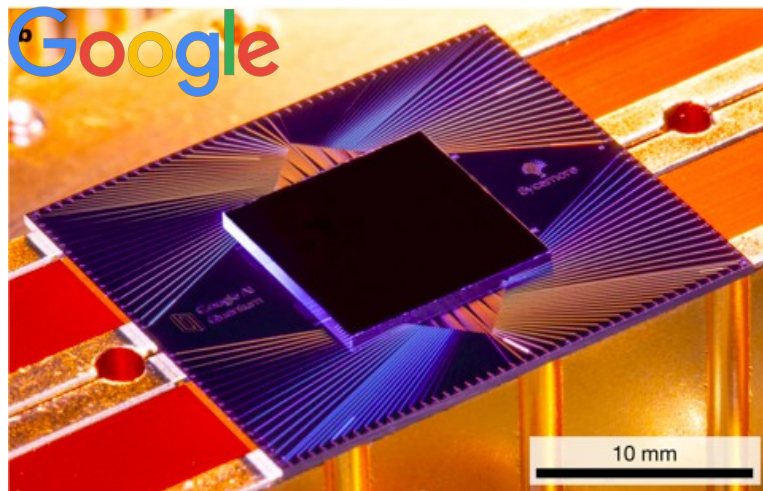
Ausztrália (UNSW):
szilíciumba ültetett
foszforatom magspinje



A hasznos kvantumszámításokhoz több millió kvantumbit kéne. Pillanatnyilag ehhez a szupravezető-alapú kvantumszámítógépek állnak legközelebb

Shor-algoritmussal prímtényezőkre bontás, $\sim 10^d : 10^d$ qubit, d^3 lépés
(Kitaev-féle módosítással, arXiv:quant-ph/9511026)

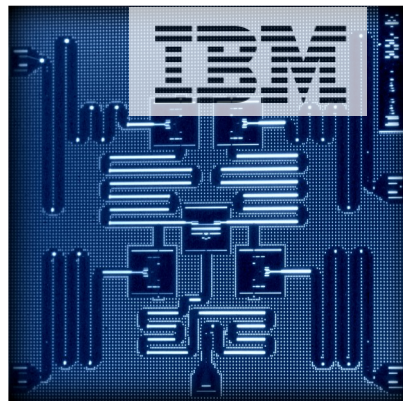
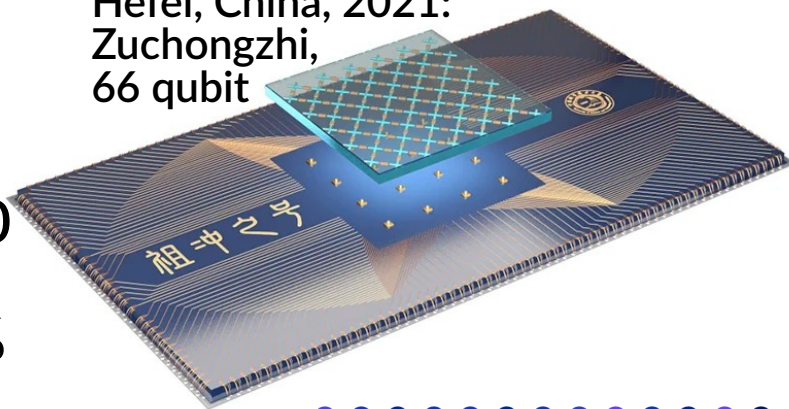
→ RSA2048 feltörése: ~ 600 számjegy:
kell 6000 qubit, 200 millió lépés → **10^{-10} pontosság**



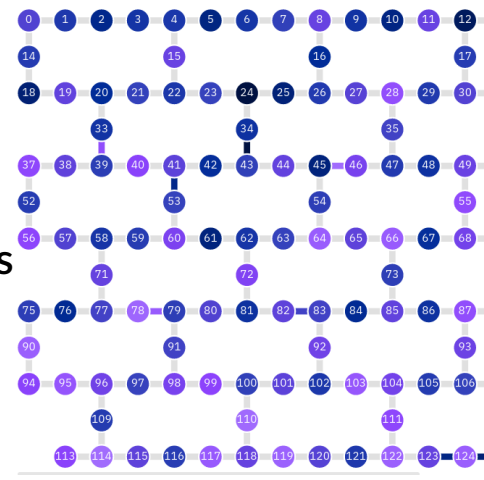
UCSB+Google, 2022:
72 qubites "Sycamore"
csipen kvantum
hibajavítás
arxiv:2207.06431 (2022)

qubitek száma ~ 100
kapuhiba: $< 1\%$
kiolvasási hiba: $\sim 2\%$

Hefei, China, 2021:
Zuchongzhi,
66 qubit

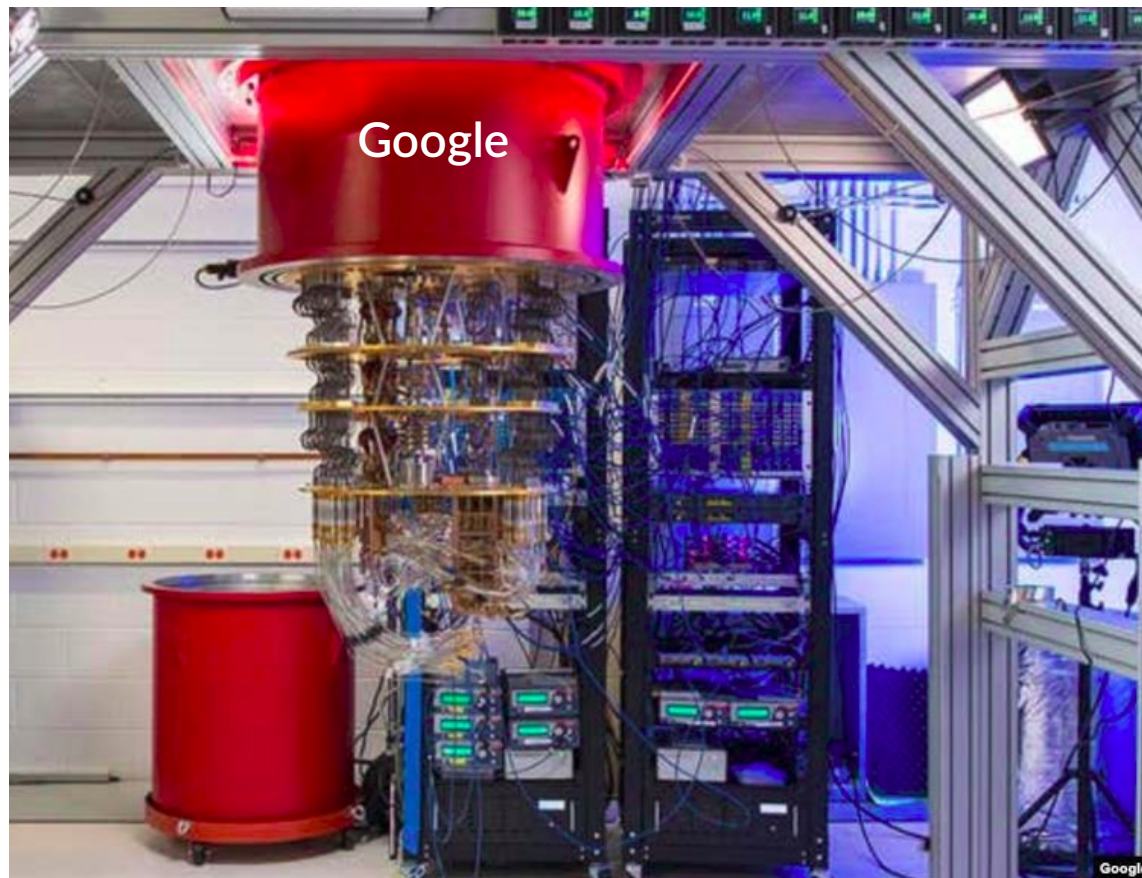


IBM, 2021:
433 qubites
"Osprey"
bejelentve,
még nem
kalibrálták



Szupravezető-alapú kvantumszámítógépek nanoáramköröit 10 mK körülre kell hűteni, hogy a környezet zavaró hatásait kiszűrjék

Egész áramkört hűteni nehezebb, mint néhány iont

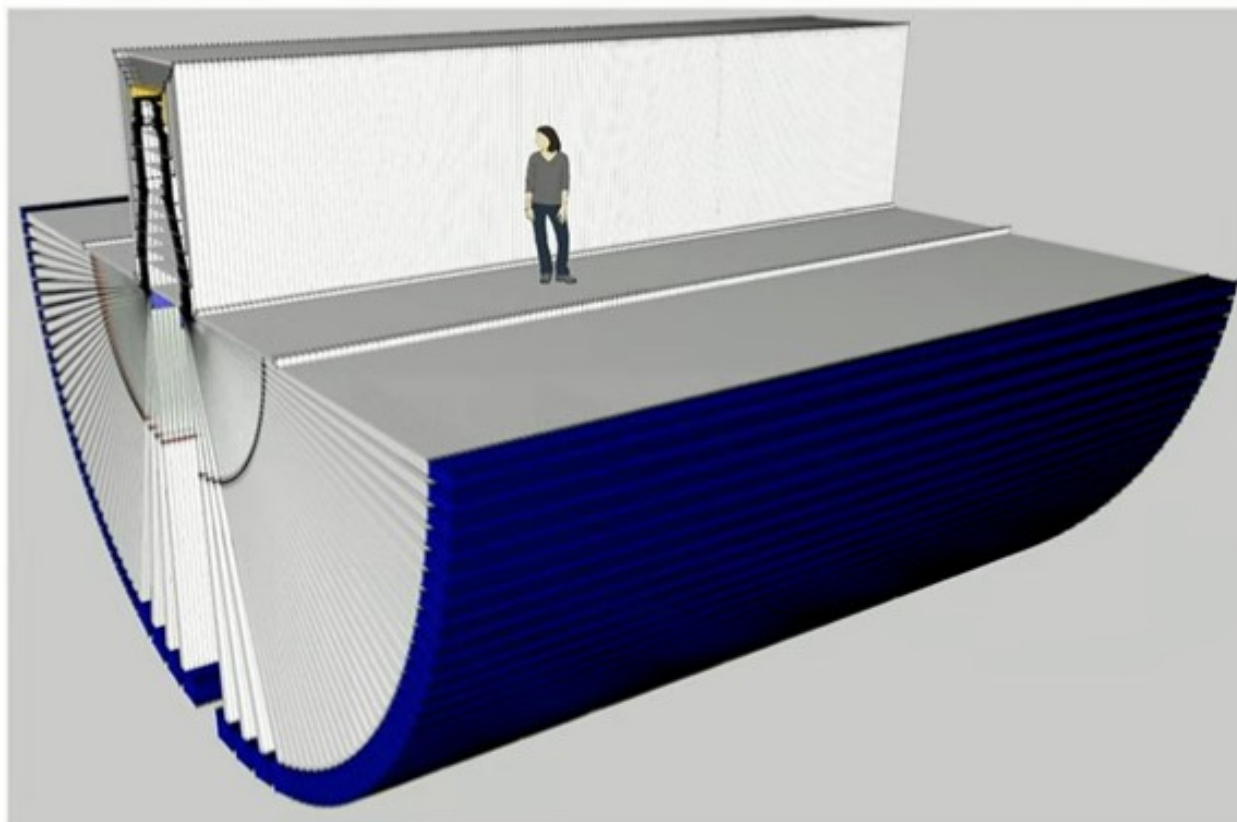


He3/He4 keveréses hűtő (1 millió \$) → 15 mK (200x hidegebb a csillagközi térnél).

Magyarországon: BME Kvantumelektronika Csoport <https://nanoelectronics.physics.bme.hu/>

A Google és az IBM is 2030-ra 1 millió kvantumbites számítógépet ígér

10^6 qubit milestone: Error-corrected quantum computer



2048-bit RSA :
1 hour,
20M qubits

4096-bit RSA :
2 hours,
40M qubits

65536-bit RSA:
4 days,
1000M qubits

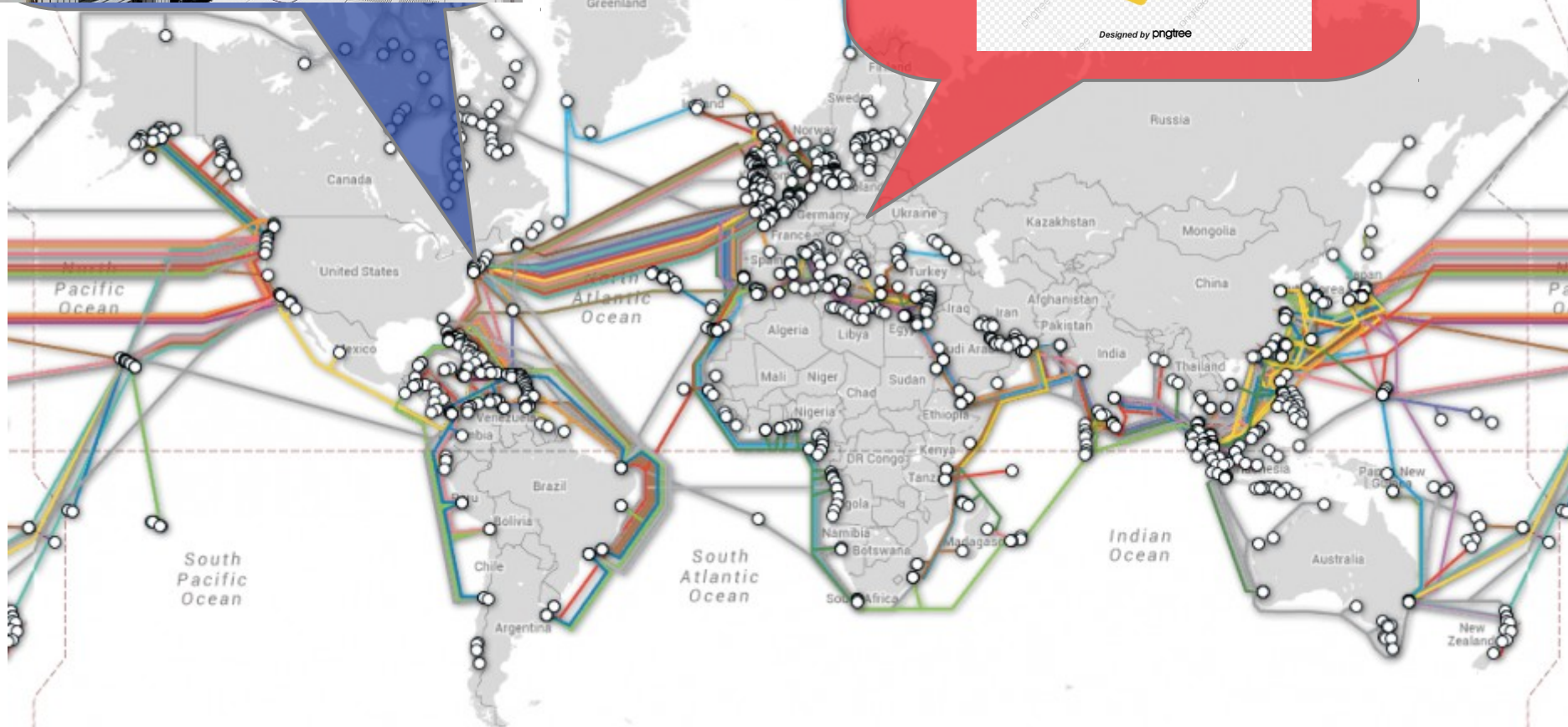
Consists of
~100 tiled modules

Tiles consist of
~100x100 physical qubits

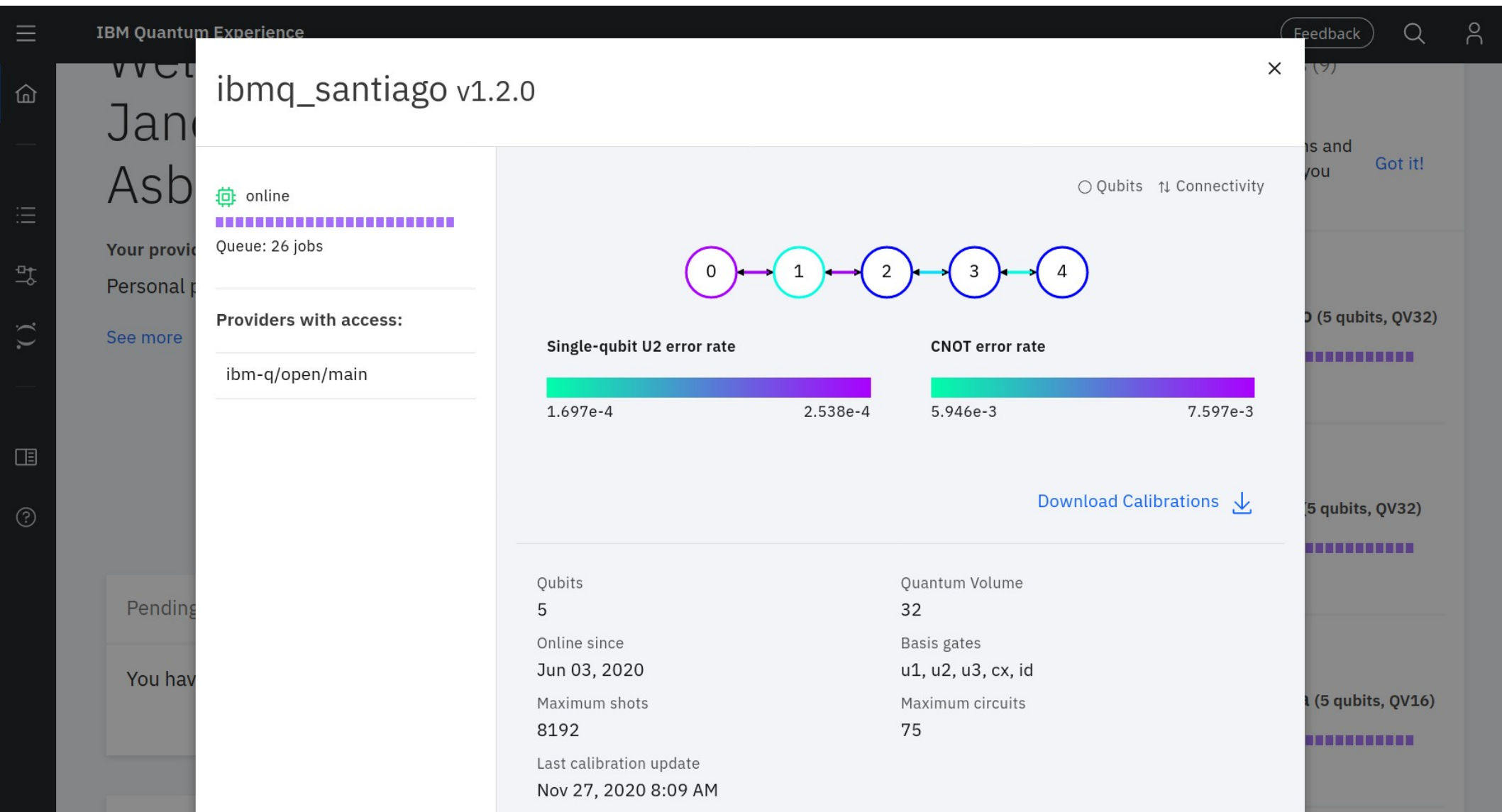
[Gidney & Eker: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, arXiv:1905.09749]

[Hartmut Neven's talk on Google Summer Symposium 2020,
<https://www.youtube.com/playlist?list=PLQY2H8rRoyvx4VttfJOPRslw8XWT7yaBJ>]

Az IBM Quantum Experience online hozzáférést ad kvantumszámítógépekhez



Az IBM gépparkjáról naprakész információt ad az online felületük (naponta újrakalibrált kvantumszámítógépek)

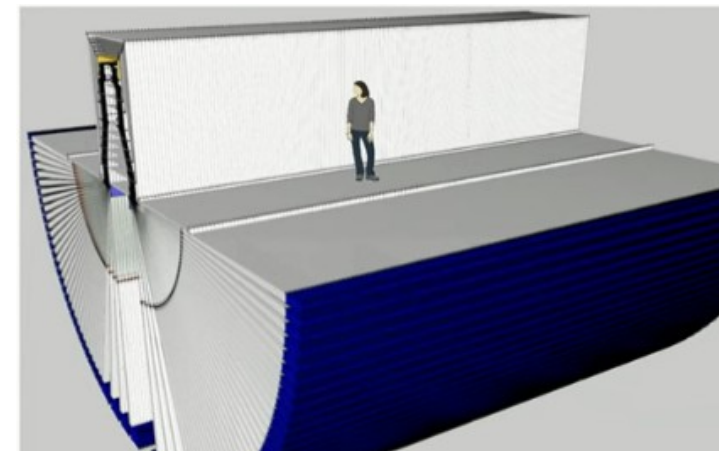
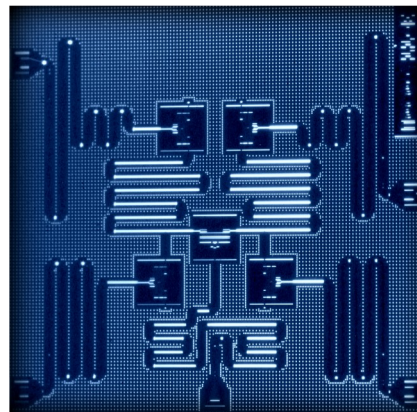
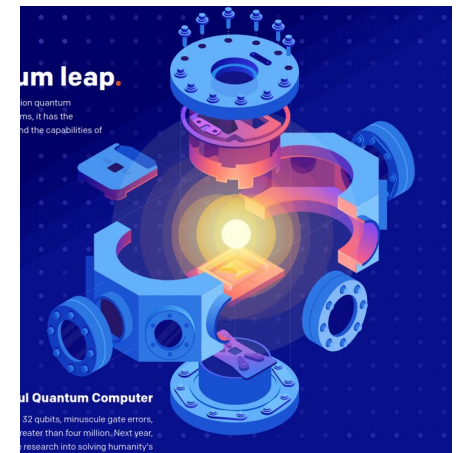


A kvantumszámítógépek mindjárt itt vannak.
Tanuljuk meg használni őket!

- Kvantumbitek superpozícióban:
Kvantumlogikai kapuk (NOT, Z, H, CNOT)
- Igazán hasznos kvantumszámítógép még nincs:
~1 millió kvantumbit, ~0.1% kapuhiba, kiolvasási hiba
 - titkosítás feltörése, kvantumkémia
 - quantumalgorithmzoo
- Természetadta kvantumbitek:
vákuumkamrában lebegtetett ionok
- Legígéretesebb hardver:
szupravezető nanoáramkörök
(kvantumfölény benchmark 2019:
véletlen kvantumos logikai áramkör
mintavételezése)
- Programozásra fel!
IBM Quantum Experience

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$\begin{aligned} \text{---} \boxed{Z} \text{---} &= \text{---} \boxed{H} \oplus \boxed{H} \text{---} \\ \text{---} \oplus \text{---} &= \text{---} \boxed{H} \boxed{Z} \boxed{H} \text{---} \end{aligned}$$









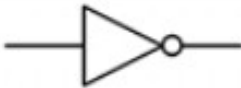
Programozás alapjai: bitek

digits position	5	4	3	2	1	0
binary	1	0	0	0	1	0
	$32 = 1 \times 2^5$	$0 = 0 \times 2^4$	$0 = 0 \times 2^3$	$0 = 0 \times 2^2$	$2 = 1 \times 2^1$	$0 = 0 \times 2^0$
decimal	$32 + 0 + 0 + 0 + 2 + 0 = 34$					

Decimal	Binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111







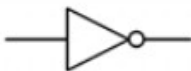
Írd fel az életkorod bináris számmal! Add össze a szomszédodéval, írd fel azt is! Ellenőrizzétek egymás eredményét

Programozás alapjai: bitek, és rajtuk ható logikai áramkörök

Logic Gate	Symbol	Description	Boolean
AND		Output is at logic 1 when, and only when all its inputs are at logic 1, otherwise the output is at logic 0.	$X = A \cdot B$
OR		Output is at logic 1 when one or more are at logic 1. If all inputs are at logic 0, output is at logic 0.	$X = A + B$
NAND		Output is at logic 0 when, and only when all its inputs are at logic 1, otherwise the output is at logic 1	$X = \overline{A \cdot B}$
NOR		Output is at logic 0 when one or more of its inputs are at logic 1. If all the inputs are at logic 0, the output is at logic 1.	$X = \overline{A + B}$
XOR		Output is at logic 1 when one and Only one of its inputs is at logic 1. Otherwise is it logic 0.	$X = A \oplus B$
XNOR		Output is at logic 0 when one and only one of its inputs is at logic 1. Otherwise it is logic 1. Similar to XOR but inverted.	$X = \overline{A \oplus B}$
NOT		Output is at logic 0 when its only input is at logic 1, and at logic 1 when its only input is at logic 0. That's why it is called and INVERTER	$X = \overline{A}$

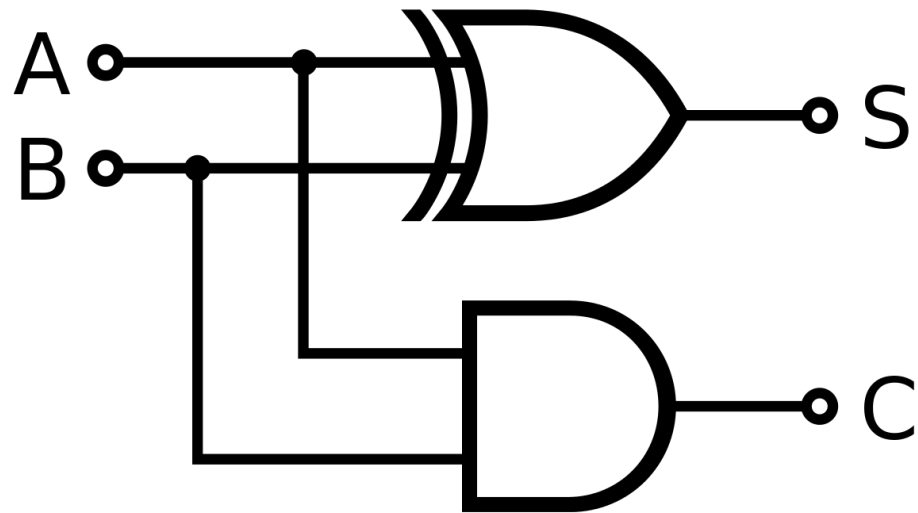
Pl. két bit összeadása: hogyan kell megcsinálni?

$$\begin{array}{cccc}
 0+0=0 & 0+1=1 & 1+0=1 & 1+1=10=1*2+0 \\
 00 & 01 & 01 & 10
 \end{array}$$

Logic Gate	Symbol	Description	Boolean
AND		Output is at logic 1 when, and only when all its inputs are at logic 1, otherwise the output is at logic 0.	$X = A \cdot B$
OR		Output is at logic 1 when one or more are at logic 1. If all inputs are at logic 0, output is at logic 0.	$X = A + B$
NAND		Output is at logic 0 when, and only when all its inputs are at logic 1, otherwise the output is at logic 1	$X = \overline{A \cdot B}$
NOR		Output is at logic 0 when one or more of its inputs are at logic 1. If all the inputs are at logic 0, the output is at logic 1.	$X = \overline{A + B}$
XOR		Output is at logic 1 when one and Only one of its inputs is at logic 1. Otherwise is it logic 0.	$X = A \oplus B$
XNOR		Output is at logic 0 when one and only one of its inputs is at logic 1. Otherwise it is logic 1. Similar to XOR but inverted.	$X = \overline{A \oplus B}$
NOT		Output is at logic 0 when its only input is at logic 1, and at logic 1 when its only input is at logic 0. That's why it is called and INVERTER	$X = \overline{A}$

<https://circuitverse.org/simulator>

Pl. két bit összeadása: megoldás



A kvantumbit: szuperpozícióban is tud lenni

abstract

$|0\rangle$

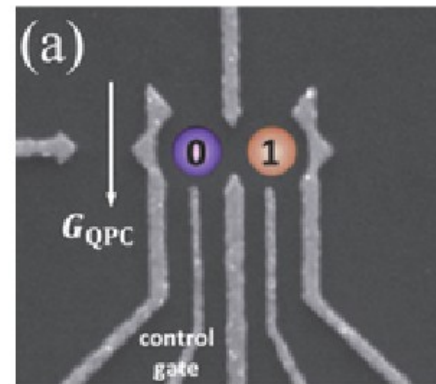
$|1\rangle$

spin

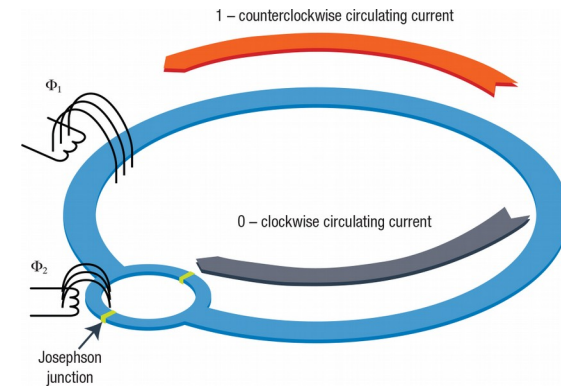
$|\uparrow\rangle$

$|\downarrow\rangle$

charge



superconducting current



Superposition:

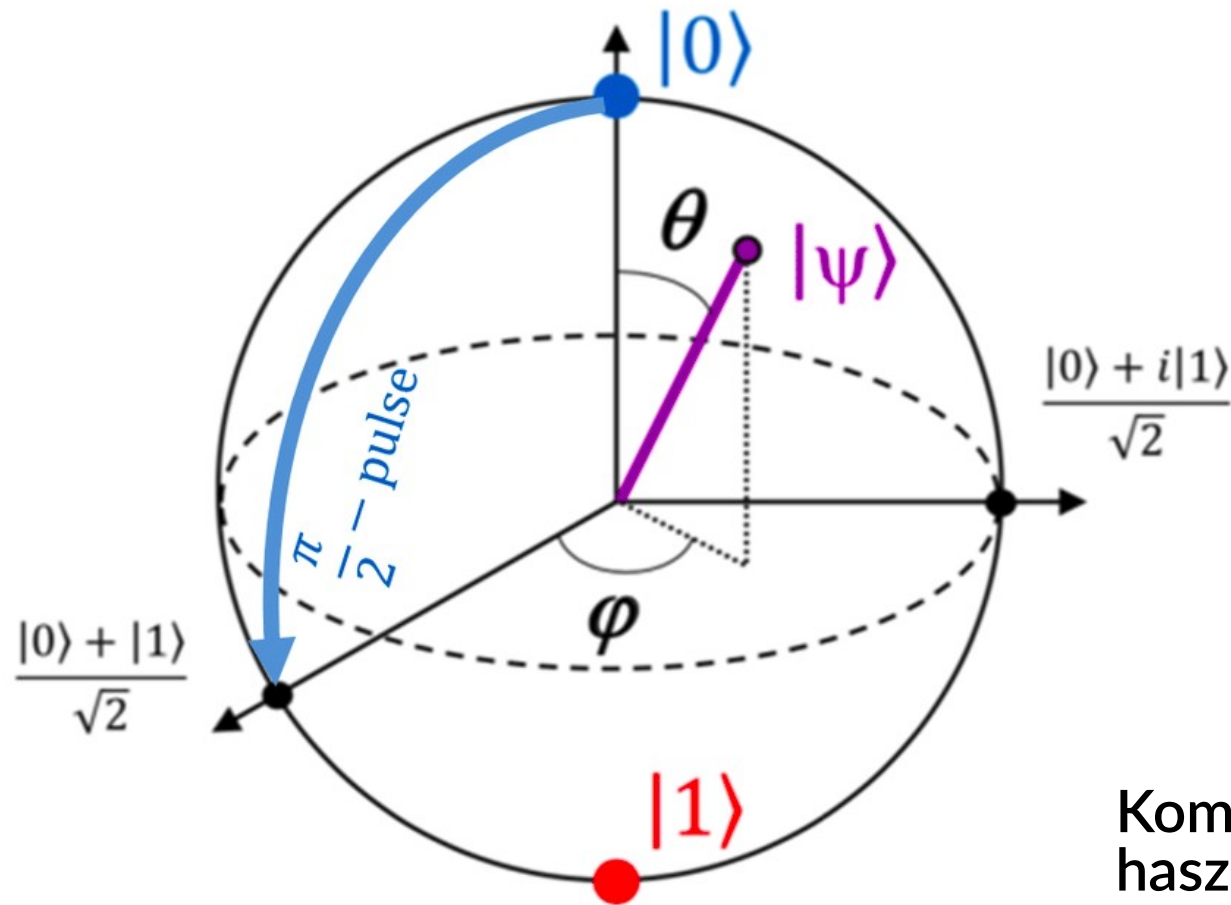
$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Measurement produces 1 or 0, probabilistically

$$|\Psi\rangle \longrightarrow \begin{cases} |\alpha|^2 \rightarrow 0 \\ |\beta|^2 \rightarrow 1 \end{cases}$$

[Mooij, Delft, 2001]

Egy db. kvantumbit összes lehetséges szuperpozíciós állapota: két pont helyett egy gömb felszíne



Komplex számok
használatával
könnyen felírható

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

Hasonlóan a hagyományos számítógépekhez, kvantumszámítógépekben is logikai kapuk vannak.

Defined as classical NOT (bit flip):

$$|0\rangle \xrightarrow{\oplus} |1\rangle$$

$$|1\rangle \xrightarrow{\oplus} |0\rangle$$

Action on superposition states:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi\rangle \xrightarrow{\oplus} \beta|0\rangle + \alpha|1\rangle$$

Purely quantum gate,
changes phase:

$$|0\rangle \xrightarrow{\square Z} |0\rangle$$

$$|1\rangle \xrightarrow{\square Z} -|1\rangle$$

Action on superposition states:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi\rangle \xrightarrow{\square Z} \alpha|0\rangle - \beta|1\rangle$$

A Hadamard-kapu szuperpozícióba hozza a kvantumbitet

Bázisállapotból
szuperpozíciót hoz létre

$$\begin{aligned} |0\rangle &\xrightarrow{\text{H}} |0\rangle + |1\rangle & \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ |1\rangle &\xrightarrow{\text{H}} |0\rangle - |1\rangle & \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned}$$

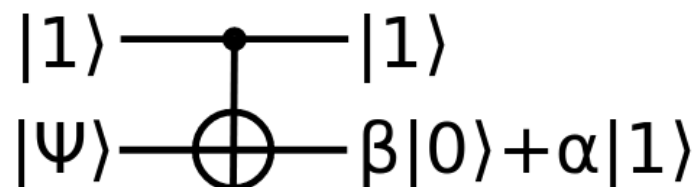
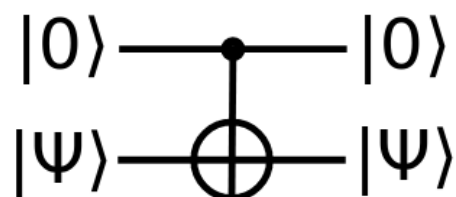
Általános állapotból:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

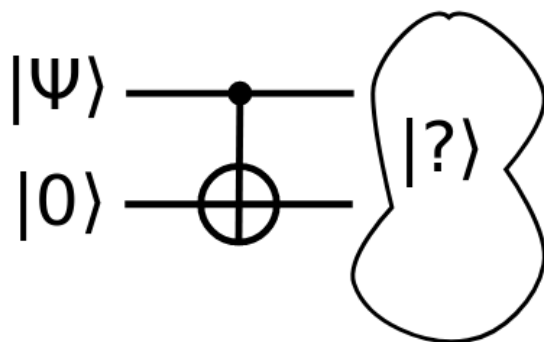
$$H|\Psi\rangle = \frac{\alpha}{\sqrt{2}} (|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{\alpha + \beta}{\sqrt{2}} |0\rangle + \frac{\alpha - \beta}{\sqrt{2}} |1\rangle$$

Hasonlóan a NAND-kapuhoz, szükség van kétbites kvantum logikai kapura is. Ilyen a CNOT

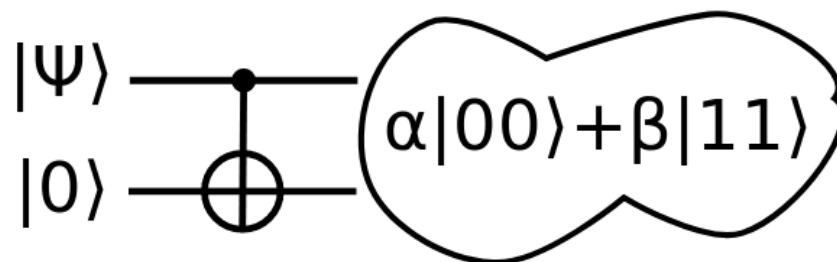
Defined for simple values of control bit,
arbitrary target bit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$



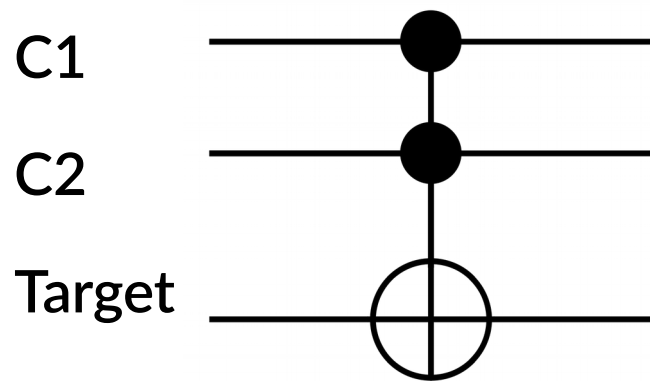
Is it a quantum copier?



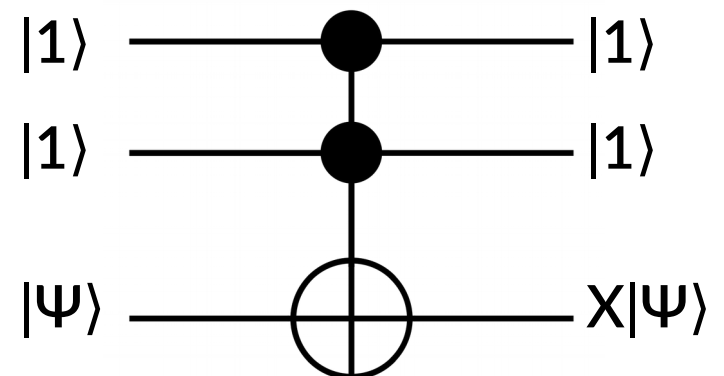
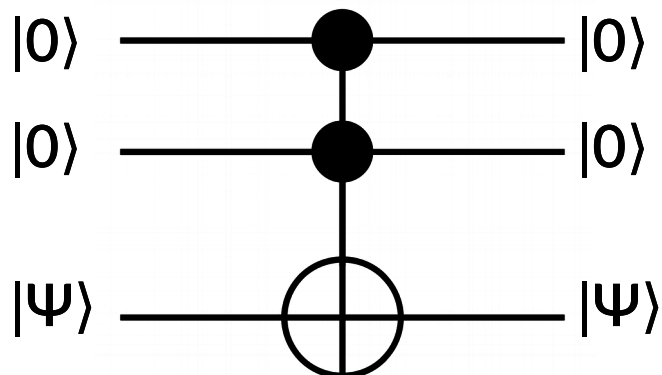
No, it is a quantum entangler



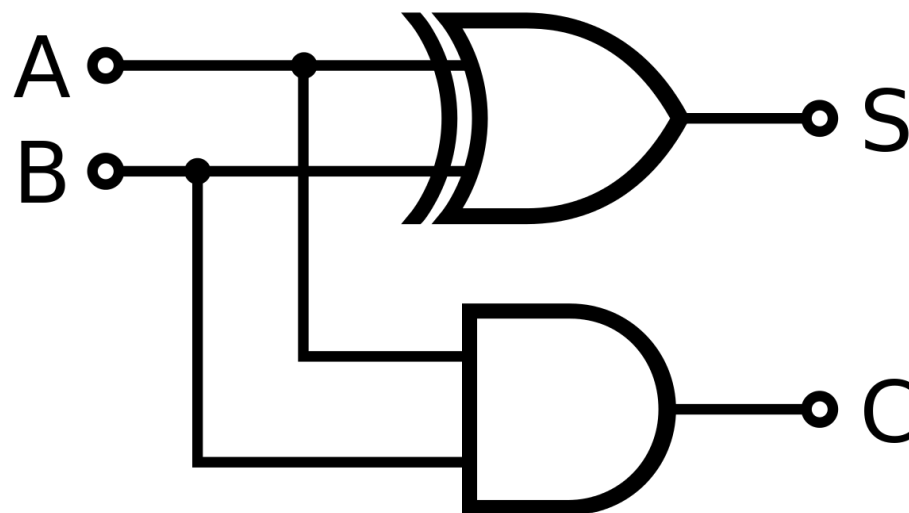
Még egy hasznos kvantumlogikai kapu: a kétszeresen vezérelt billentő kapu, Toffoli-kapu



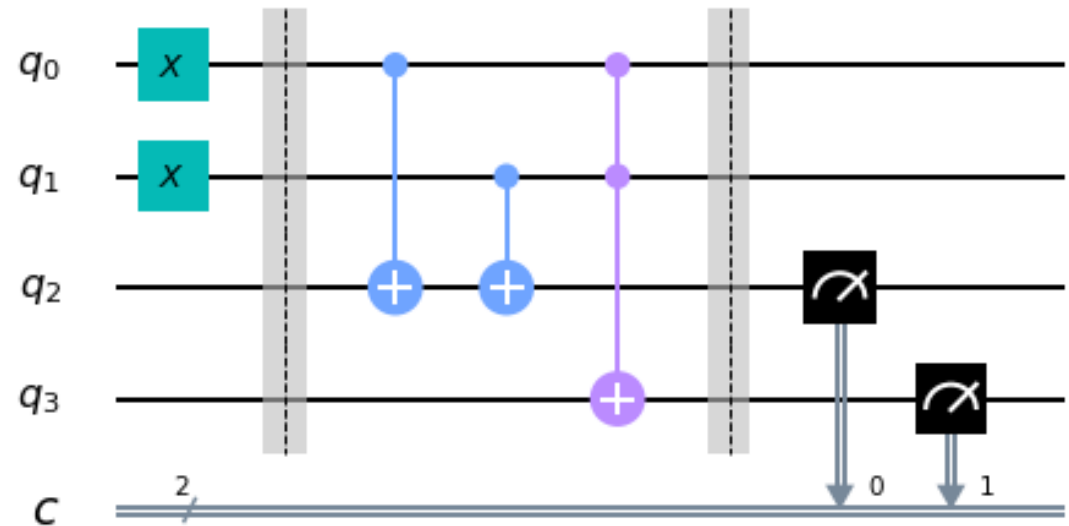
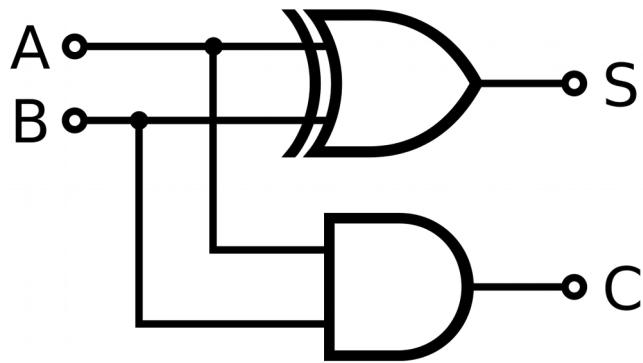
Hatása: NOT a
Target biten, csak
ha C1 és C2 is 1
állapotú



Hogyan kell a bit-összeadó áramkört megcsinálni kvantumlogikai áramkörrel?



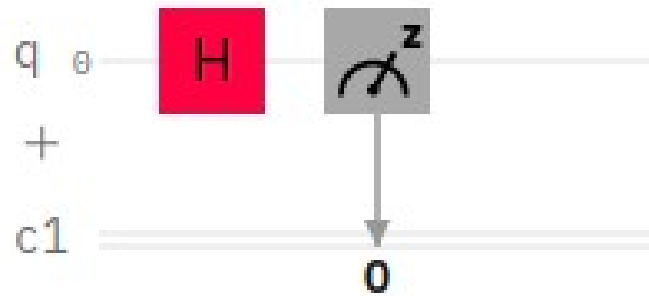
Hogyan kell a bit-összeadó áramkört megcsinálni kvantumlogikai áramkörrel?



Ellenőrizzük le az IBM Quantum Composeren!

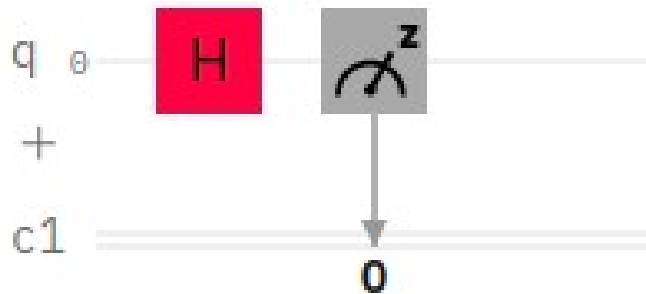
<https://quantum-computing.ibm.com/composer/docs/iqx/>

Mit adna ez a kvantumlogikai áramkör?



$$\begin{aligned}
 |0\rangle &\xrightarrow{H} |0\rangle + |1\rangle && \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 |1\rangle &\xrightarrow{H} |0\rangle - |1\rangle && \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned}$$

Ennek az áramkörnek a kimenetele véletlenszerű



$$\begin{aligned}
 |0\rangle &\xrightarrow{\text{H}} |0\rangle + |1\rangle & \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 |1\rangle &\xrightarrow{\text{H}} |0\rangle - |1\rangle & \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned}$$

Véletlen kimenetelű kísérlet: p a siker valószínűsége,
 N ismétlésből k siker vszínűsége:

$$p_k = \frac{N!}{k!(N-k)!} p^k (1-p)^{N-k}$$

Sikeres kimenetek várható k száma N kísérletből:

$$\bar{k} = Np \pm (1\dots 3) \sqrt{Np(1-p)}$$

Azonosságok – amit tudtok, számoljatok utána! Mindet ellenőrizzétek a Composerrel!

$$\text{H} \text{ H} = \text{---}$$

$$\text{H} \text{ } \oplus \text{ H} = \text{Z}$$

$$\text{H} \text{ Z} \text{ H} = \oplus$$

Swap implemented with 3 CNOTs

