

Kvantové Počítače

| Počítačová architektúra

Vypracoval: Leo Bukovčák

Obsah prednášky



História a vízia

Začiatky od Feynmanových simulácií po dnešné "Quantum Supremacy".



Fyzická vrstva

Analýza hardvérových implementácií (Supravodiče vs. Ióny vs. Fotonika).



Systémový stack

Riadiaca elektronika, kryogenika a vrstvy kvantového softvéru.



Chyby a korekcia

Dekoherencia a cesta k stabilným logickým qubitom (QEC).



Súčasnosť a Roadmap

Kde sa nachádzame dnes a aký je plán pre rok 2030.



Praktické využitie

Od chémie a materiálov k novej ére kryptografie.

Kľúčové pojmy: Čo robí PC kvantovým?



Superpozícia

- ✓ Qubit nie je len 0 alebo 1, ale oba stavy naraz.
- ✓ Umožňuje paralelne testovať miliardy riešení.
- ✓ Stav zaniká v momente merania (kolaps vlny).



Entanglement

- ✓ "Strašidelné pôsobenie na diaľku" (Einstein).
- ✓ Dva qubity sú prepojené bez ohľadu na vzdialenosť.
- ✓ Zmena stavu jedného okamžite ovplyvní druhý.



Dekoherencia

- ✓ Strata kvantových vlastností vplyvom okolia.
- ✓ Spôsobuje ju teplo, žiarenie alebo šum.
- ✓ Dôvod, prečo potrebujeme mrazivé teploty.

Teoretické základy (1980 - 1995)

Klasické počítače sú neefektívne pri simulácii kvantových systémov.

- ✓ **1981:** Richard Feynman navrhuje kvantový simulátor.
- ✓ **1985:** David Deutsch definuje Univerzálny kvantový počítač.
- ✓ **1994:** Peter Shor publikuje algoritmus na faktorizáciu čísel (hrozba pre RSA).
- ✓ **1996:** Lov Grover definuje algoritmus pre rýchle vyhľadávanie v databázach.

"Príroda nie je klasická, sakra, a ak ju chcete simulovať, radšej ju urobte kvantovo-mechanickú."

— Richard Feynman, 1981

Od laboratória ku cloudu (2000 - 2024)

2001

Shorov algoritmus spustený na
7-qubitovom NMR počítači
(faktorizácia 15).



2011

D-Wave uvádza prvý komerčný
"Quantum Annealer" (D-Wave One).



2016

IBM sprístupňuje prvý kvantový
procesor cez cloud (IBM Quantum
Experience).



2019+

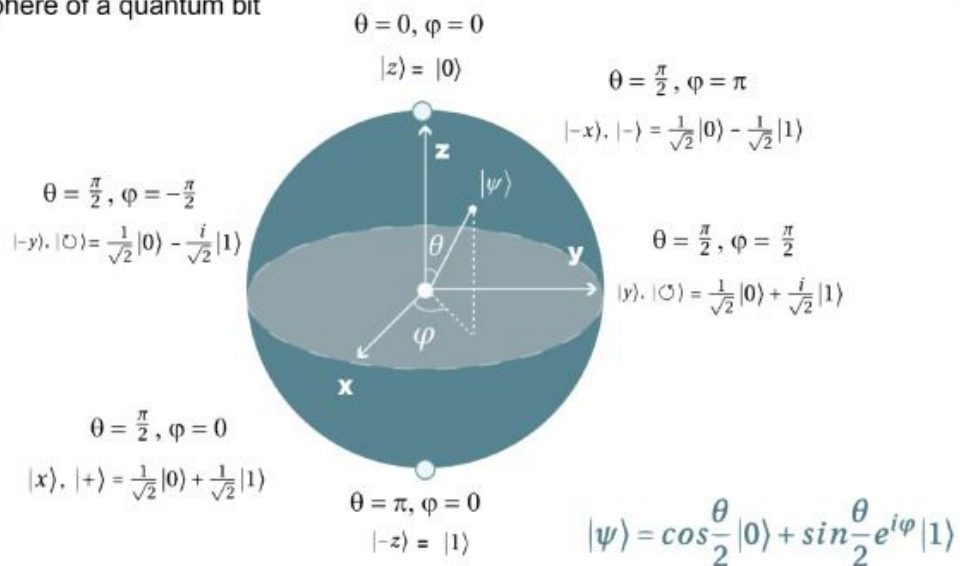
Google dosahuje "Kvantovú
nadvládu" so Sycamore
procesorom.



Prechod z **fyziky v laboratóriu** k **systemovému inžinierstvu**.

Základný blok: Architektúra qubitů

Bloch Sphere of a quantum bit



Blochova sféra

Qubit nie je len 0 alebo 1. Je to vektor v Hilbertovom priestore, reprezentovaný na povrchu sféry.

- ✓ **Superpozícia:** Stav $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- ✓ **Pravdepodobnosť:** Amplitúdy α a β určujú šancu na výsledok pri meraní
- ✓ **Fáza:** Kľúčový parameter pre interferenciu algoritmov.

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

Architektonické princípy výpočtu



Kvantová interferencia

Algoritmy sú navrhnuté tak, aby sa "nesprávne" cesty výpočtu vyrušili a tie "správne" zosilnili.



Entanglement

Neklasická korelácia medzi qubitmi. Umožňuje reprezentovať 2^n stavov naraz.



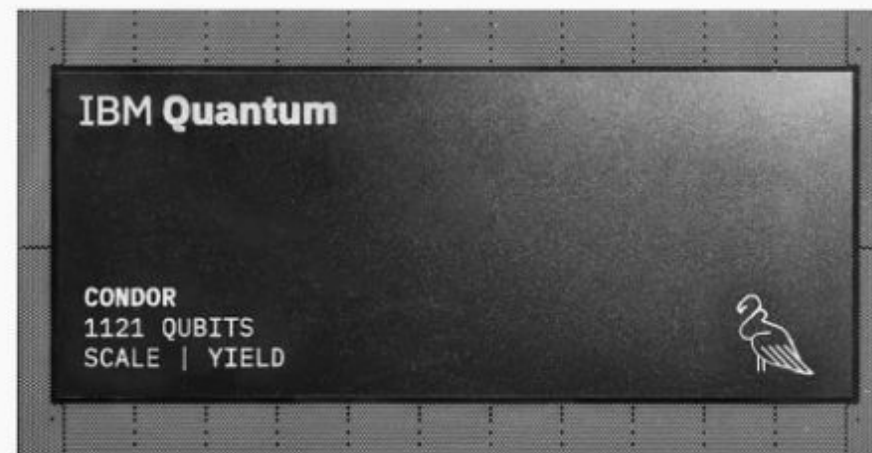
No-Cloning Theorem

Kvantovú informáciu nie je možné kopírovať. To zásadne mení spôsob prenosu dát v architektúre.

Hardvér I: Supravodivé slučky (IBM / Google)

Dnes najrozšírenejšia architektúra založená na **Josephsonových spojoch**.

- ✓ **Transmon Qubity:** Využívajú supravodivosť na elimináciu elektrického odporu.
- ✓ **Riadenie:** Pomocou mikrovlnných pulzov v GHz pásme.
- ✓ **Výhoda:** Výroba pomocou štandardnej litografie (ako u klasických čipov).
- ✓ **Výzva:** Vyžaduje extrémne chladenie (mK) a trpí vysokým šumom.



Hardvér II: Iónové pasce (Quantinuum / IonQ)



Qubity sú jednotlivé ióny (napr. Ytterbium) uväznené v elektromagnetickom poli.

- ✓ **Riadenie:** Pomocou presne mierených laserových lúčov.
- ✓ **Vlastnosti:** Identické qubity (prírodné atómy) s dlhou dobou koherencie.
- ✓ **Konektivita:** Každý qubit môže byť prepojený s každým ("All-to-All connectivity").
- ✓ **Škálovateľnosť:** Pomalšie operačné časy a zložité optické systémy.

Full-Stack Kvantová Architektúra



QPU (Quantum Processing Unit)

Fyzické qubity (supravodiče, ióny, fotóny) na čipe.



Riadiaca elektronika

FPGA a generátory vln preklápajúce logické príkazy na pulzy.



Klasický Host

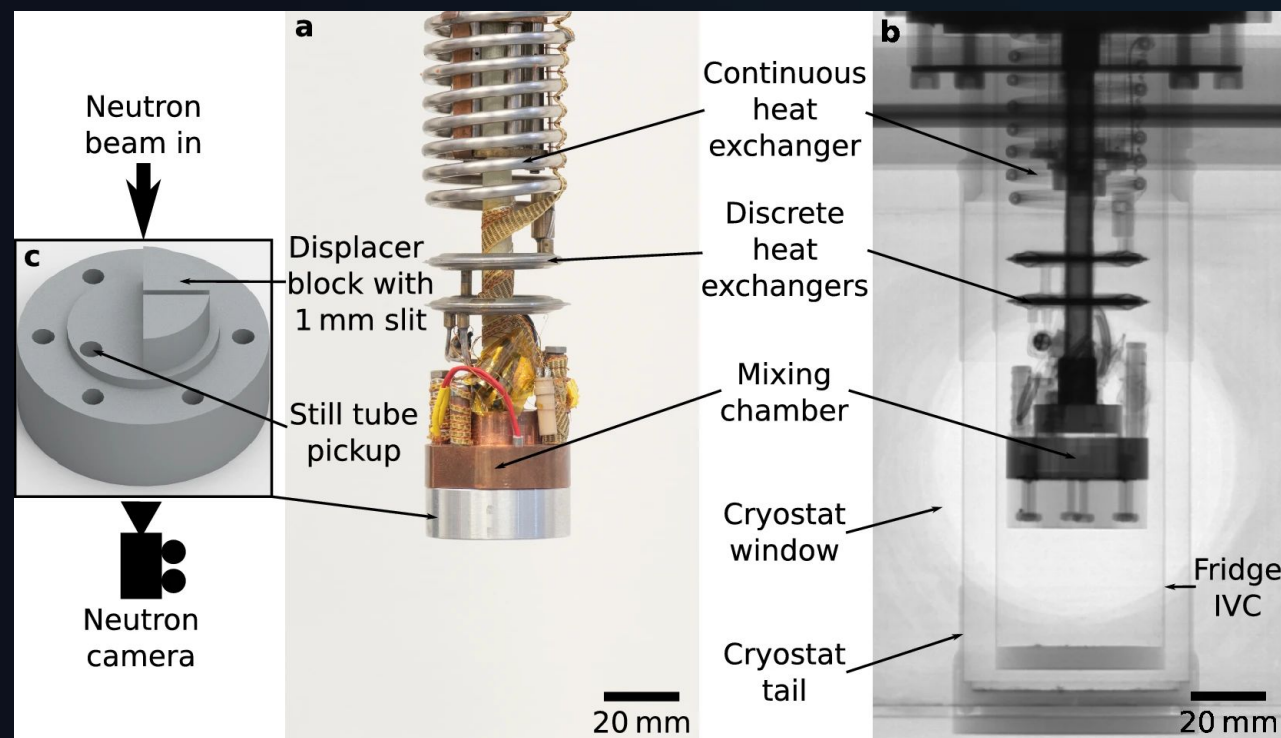
Server riadiaci sekvenciu operácií, kalibráciu a spracovanie výsledkov.

Kľúčová rola hybridných systémov: Väčšina dnešných výpočtov prebieha v cykle medzi QPU a klasickým CPU (napr. VQE algoritmy).

Infraštruktúra: Kryogenické prostredie

Pre supravodivé qubity je teplota kritickým faktorom stability.

- ✓ **Dilution Refrigerator:** Znižuje teplotu na cca **15 mK** (chladnejšie ako v hlbokom vesmíre).
- ✓ **Tienenie:** Ochrana pred magnetickým poľom Zeme a infračerveným žiarením.
- ✓ **I/O Kabeláž:** Špeciálne koaxiálne káble prenášajúce signály bez prenosu tepla.



Najväčšia výzva: Šum a dekoherencia

10⁻³

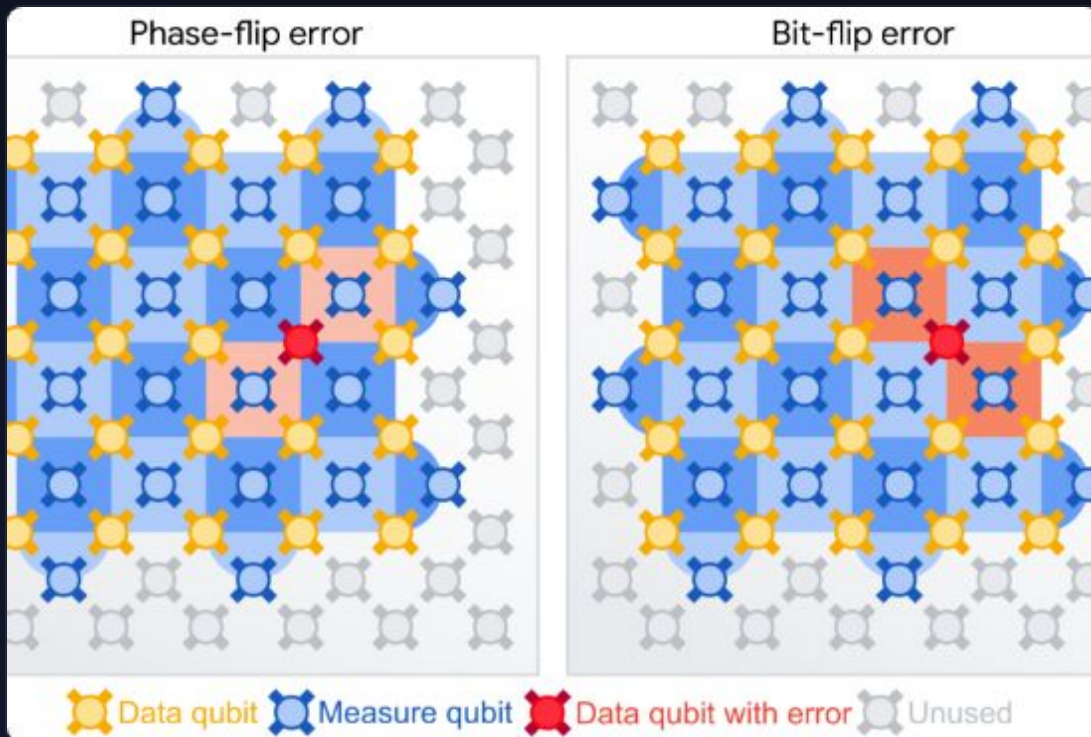
Chybovosť 2-qubitových brán

Prečo je to problém?

V klasickom počítači je chybovosť takmer nulová . V kvantovom svete:

- ✓ **T1 (Relaxácia):** Čas, kým qubit spontánne spadne zo stavu 1 do 0.
- ✓ **T2 (Defázovanie):** Čas, kým sa stratí fázová informácia qubit.
- ✓ **Šum prostredia:** Vibrácie, teplota aj kozmické žiarenie ničia výpočet.

Riešenie: Oprava chýb (QEC)



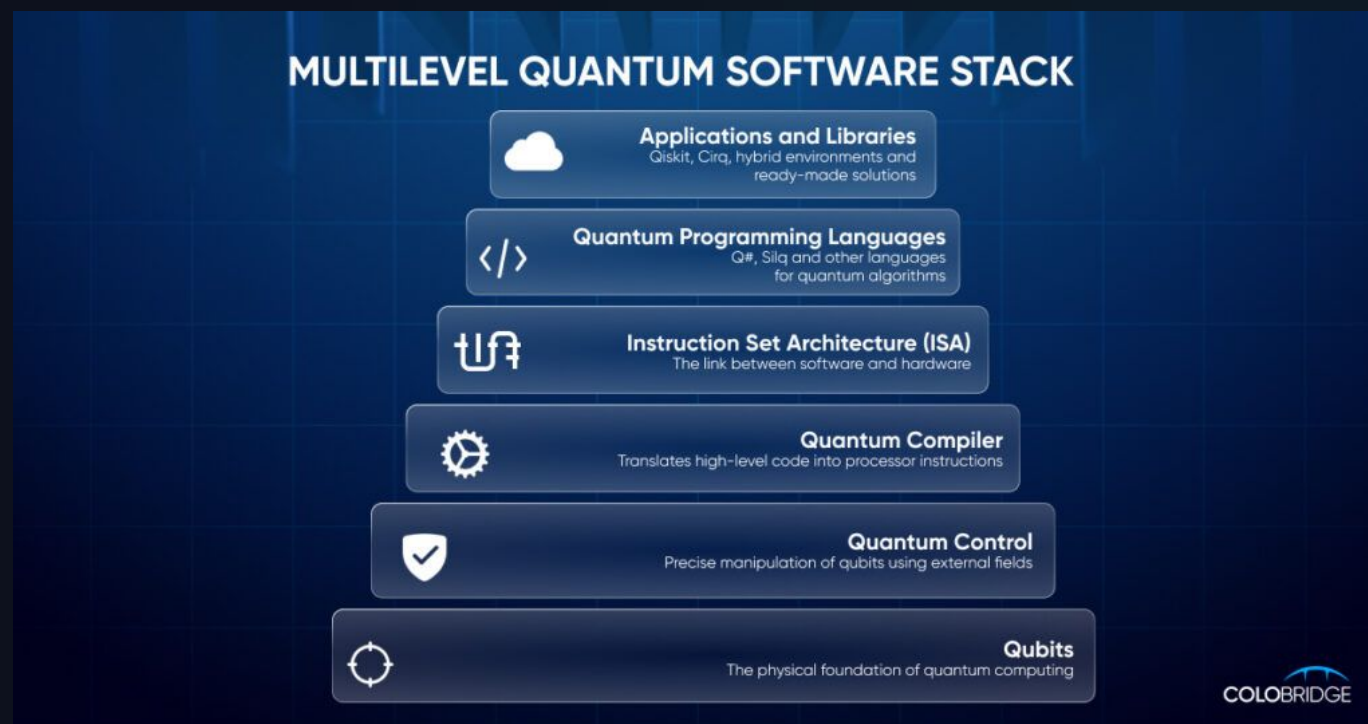
Cesta od **fyzických** qubitov k **logickým** qubitom.

- ✓ **Surface Code:** Mriežka qubitov, kde sú dáta rozložené medzi viaceré fyzické jednotky.
- ✓ **Syndrome Measurement:** Neustále kontrolovanie stavu bez zničenia superpozície dát.
- ✓ **Režijný náklad:** Na 1 logický qubit môžeme potrebovať stovky až tisíce fyzických qubitov.

Microsoft a Quantinuum nedávno demonštrovali 4 logické qubity s 800× nižšou chybovosťou.

Softvérový Stack a Vrstvy Abstrakcie

- ✓ **Aplikačná vrstva:** Problémy chémie, financií, ML (napr. PennyLane).
- ✓ **Algoritmická vrstva:** High-level programovanie (Qiskit, Cirq, Q#).
- ✓ **Kompilácia a Optimalizácia:** Redukcia počtu brán pre špecifický hardvér.
- ✓ **QASM (Quantum Assembly):** Jazyk nízkej úrovne definujúci kvantové obvody.
- ✓ **Firmware / Pulzy:** Priame riadenie fyzických qubitov.



Programovanie v Qiskite (Python)

Qiskit je open-source SDK od IBM, ktoré prekladá kód na kvantové operácie.

- ✓ **Circuit (Obvod):** Mapa inštrukcií pre qubity.
- ✓ **H-brána:** Vytvorí superpozíciu.
- ✓ **CX-brána:** Previaže dva qubity (Entanglement).
- ✓ **Simulátory vs Realita:** Kód môže bežať na vašom PC alebo cez cloud na reálnom HW.

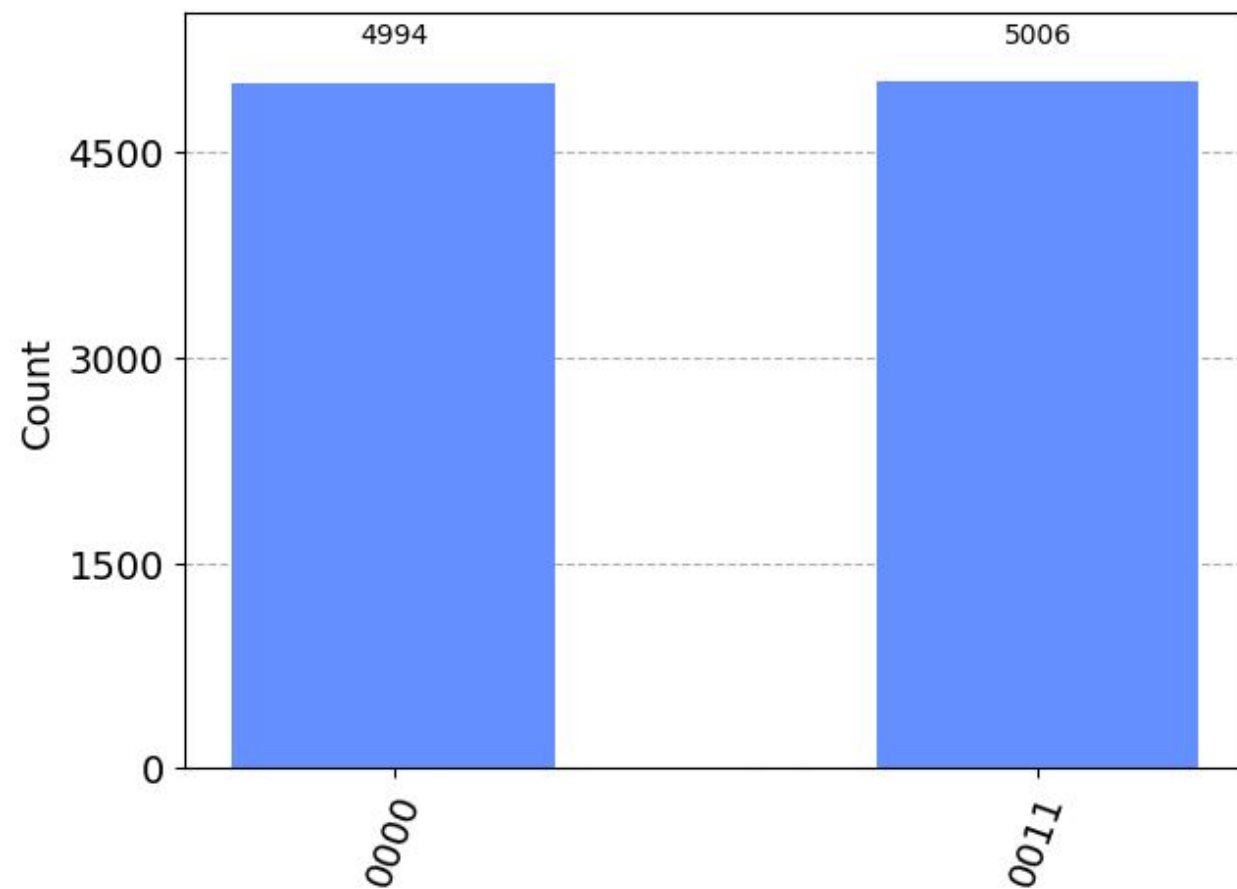
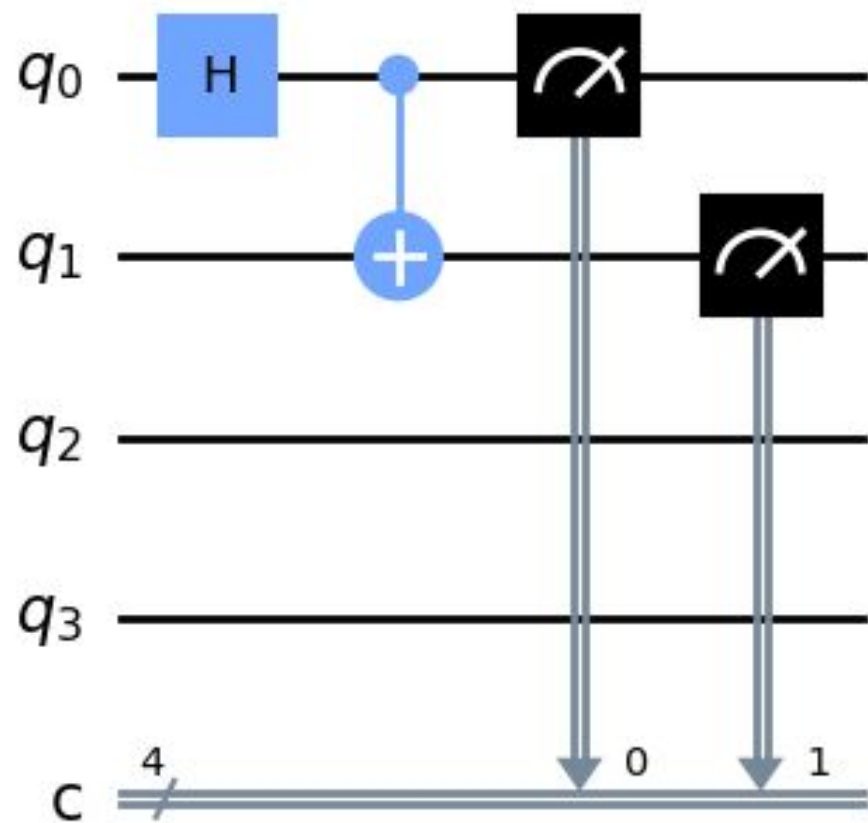
```
from qiskit import QuantumCircuit

# 1. Vytvoríme obvod s 2 qubitmi
qc = QuantumCircuit(2)

# 2. Aplikujeme Hadamardovu bránu (H)
qc.h(0)

# 3. Previažeme (CNOT)
qc.cx(0, 1)

# 4. Zmeriame výsledky
qc.measure_all()
```



Kvantový Softvérový Stack



Aplikácie

Python, Qiskit, Q#, PennyLane.



Kompilátor

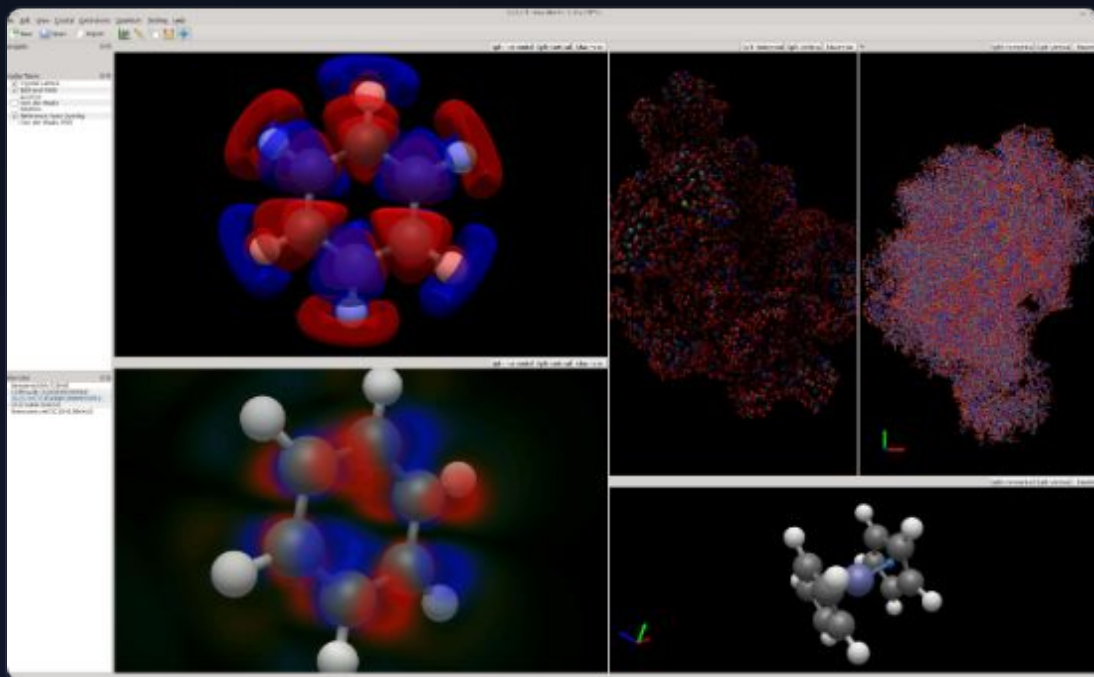
Optimalizuje počet brán, aby sa znížil šum.



Hardvér

Supravodiče, Ióny alebo Fotonika.

Praktické aplikácie architektúry



Kvantová simulácia

Presné modelovanie molekúl pre lieky a batérie. Klasické počítače tu narážajú na exponenciálnu bariéru.

- ✔ **Kryptografia:** Shorova faktorizácia a Post-kvantové štandardy (PQC).
- ✔ **Optimalizácia:** Logistika, investičné portfóliá (Monte Carlo simulácie).
- ✔ **Materiálové vedy:** Hľadanie supravodičov pri izbovej teplote.

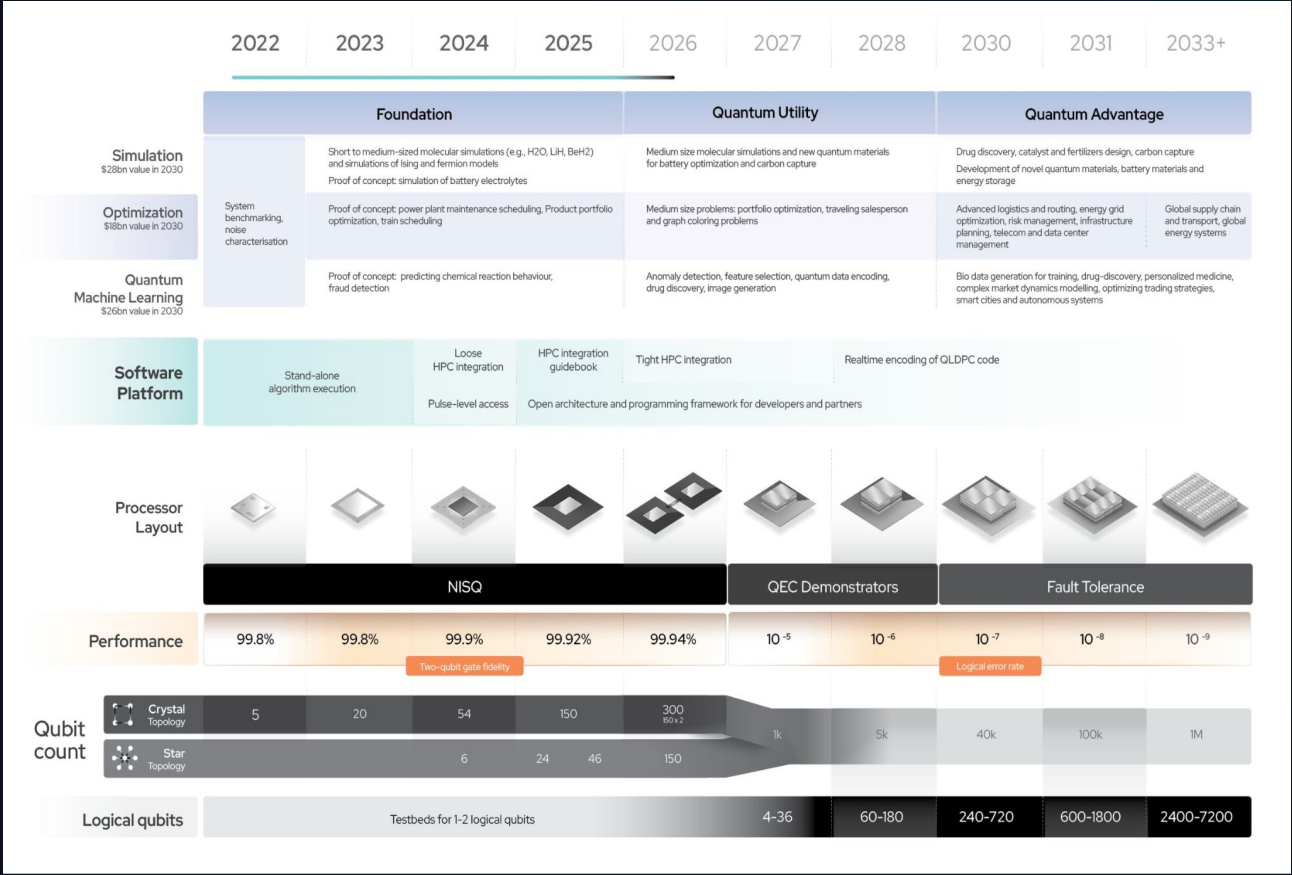
Súčasný stav HW technológií

Architektúra	Hlavní hráči	Počet Qubitov (2024)	Fidelita (Vernosť)
Supravodiče	IBM, Google, Rigetti	1121+ (IBM Condor)	~99.9% (2-qubit)
Iónové pasce	Quantinuum, IonQ	30 - 60	~99.99% (Top)
Neutrálne atómy	QuEra, Pasqal	256 - 1000	Rýchlo rastie
Fotonika	PsiQuantum, Xanadu	Škálovateľné (módy)	Variabilná

Roadmapa do roku 2030

Prechádzame z éry **NISQ** (Noisy Intermediate-Scale Quantum) do éry **Fault-Tolerant**.

- 2024–2025: Demonštrácia prvých užitočných logických qubitov.
- 2026–2028: Prekonanie klasických superpočítačov v praktických úlohách.
- 2030+: Milióny fyzických qubitov pracujúcich v sieti (Quantum Internet).



Závery a kľúčové body

- ✓ Kvantová architektúra nie je náhradou klasickej, ale jej **zlepšením** pre špecifické úlohy.
- ✓ Hardvérový závod: Nie je jasné, ktorá technológia (supravodiče vs ióny) zvíťazí.
- ✓ Kľúčom k úspechu je **Error Correction** – bez neho zostanú kvantové počítače len vedeckým experimentom.
- ✓ Softvérový ekosystém je už pripravený, čaká sa len na stabilnejší hardvér.
- ✓ Príprava na "Q-Day" – moment, kedy kvantové stroje ohrozia dnešné šifrovanie.

Otázky?

Zdroje

<https://quantum.cloud.ibm.com/docs/en/guides>

<https://meetiqm.com/resources/scientific-publications/>

<https://github.com/microsoft/quantumkatas>

<https://quantum.cloud.ibm.com/learning/en>

<https://profmcruz.wordpress.com/wp-content/uploads/2017/08/quantum-computation-and-quantum-information-nielsen-chuang.pdf>

[https://github.com/shyamsantoki/Qubit_Quantum-Computing_Notes/blob/main/Quantum%20computing%20for%20everyone%20by%20Bernhardt%2C%20Chris%20\(z-lib.org\).pdf](https://github.com/shyamsantoki/Qubit_Quantum-Computing_Notes/blob/main/Quantum%20computing%20for%20everyone%20by%20Bernhardt%2C%20Chris%20(z-lib.org).pdf)