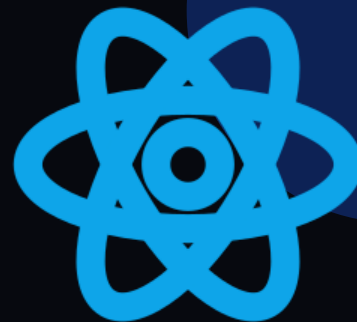


KVANTOVÉ POČÍTAČE



Od fyziky atomů k revoluci v výpočtové technice

OBSAH PREZENTÁCIE

01

História

Od Turinga po Feynmana

02

Čo je qubit?

Základ kvantového počítača

03

Kvantové javy

Superpozícia, previazanosť, interferencia

04

Ako funguje?

Hradlá, obvody, meranie

05

Fyzická realizácia

Supravodivé, iónové, fotónové

06

Klasický vs. Kvantový

Porovnanie, výhody, limity

07

Algoritmy

Shor, Grover, VQE a ďalšie

08

Aplikácie

Medicína, financie, AI, kryptografia

09

Riziká & Výzvy

Dekoherencia, bezpečnosť, etika

10

Budúcnosť

Roadmap a čo nás čaká

01

História

Ako sme sa dostali od klasických počítačov ku kvantovým?

01 | HISTÓRIA — KLÚČOVÉ MÍĽNIKY

1936

Alan Turing formuluje matematický model počítača (Turingov stroj) — základ celej informatiky.

1947

Vynález tranzistora v Bell Labs. Štart éry klasických počítačov.

1965

Gordon Moore: počet tranzistorov sa zdvojnásobuje každé 2 roky (Moorov zákon).

1980

Richard Feynman navrhuje, že fyziku možno simulovať iba kvantovým počítačom.

1982

Feynman publikuje esej o kvantových počítačoch — prvý teoretický opis.

1985

David Deutsch definuje univerzálny kvantový počítač — formálny matematický základ.

1994

Peter Shor objavuje algoritmus na faktorizáciu čísel — prelom v kryptografii.

1996

Lov Grover: kvantový vyhľadávací algoritmus (VN zrýchlenie).

1998

Prvý 2-qubitový kvantový počítač v laboratóriu (NMR technológia).

2019

Google: 'kvantová nadvláda' — Sycamore (54 qubitov) zvládol úlohu za 200 sekúnd (superpočítač by potreboval 10 000 rokov).

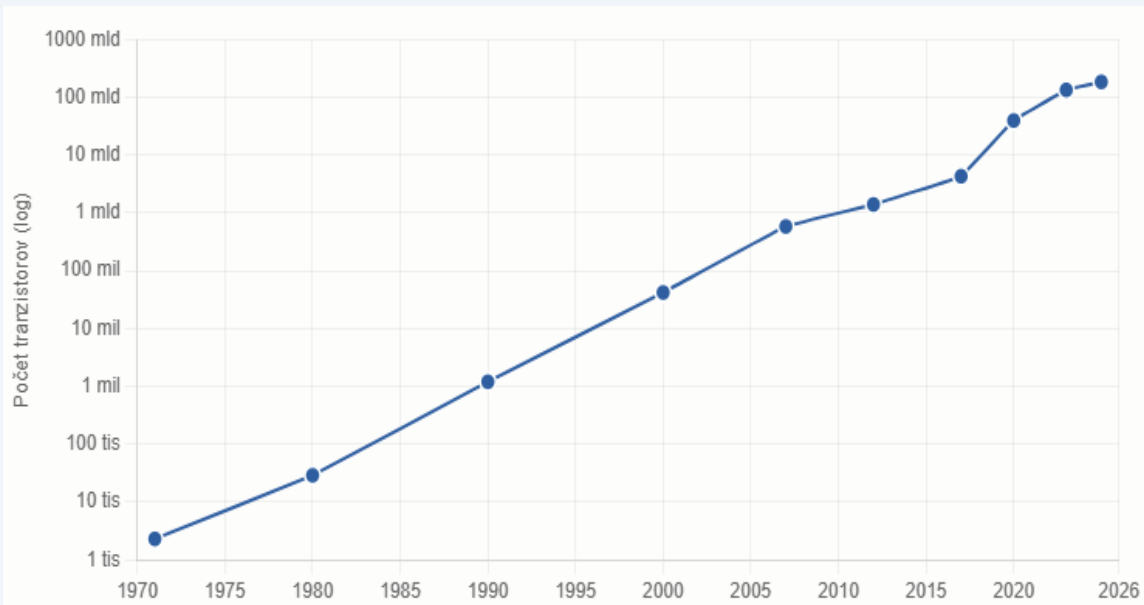
2023

IBM Condor: 1 121 fyzických qubitov. Závod o chybovo odolné kvantové počítače pokračuje.

2024

Google Willow: prelom v oprave chýb. NIST vydáva post-quantové kryptografické štandardy.

Prečo klasické počítače nestačia?



Fyzikálny limit

Tranzistory dnes ~2 nm — blížíme sa k atomárnym rozmerom. Kvantové efekty rušia klasickú logiku.



Energetická kríza

Dátové centrá spotrebúvajú ~2 % celosvetovej elektriny. Klasická škálovateľnosť naráža na limity.



Exponenciálna zložitosť

Mnohé problémy (optimalizácia, AI, simulácia) rastú exponenciálne — klasický HW jednoducho nestačí.

02

Čo je Qubit?

Základná jednotka kvantovej informácie

02 | BIT vs. QUBIT — ZÁKLADNÝ ROZDIEL



Klasický BIT

- Môže byť iba 0 alebo 1
- Deterministická hodnota
- Ľahko čitateľný
- Základná operácia (logické hradlá)
: AND, OR, NOT
- n bitov = 1 z 2^n možných stavov
- Funguje pri izbovej teplote
- Realizácia: tranzistor (ON/OFF)

VS



Kvantový QUBIT

- Môže byť 0, 1 alebo oboje naraz (superpozícia)
- Pravdepodobnostný — meranie ho 'zrúti'
- Meranie zničí kvantový stav
- Kvantové hradlá: H, CNOT, Toffoli...
- n qubitov = 2^n stavov súčasne
- Potrebuje ~ 15 millikelvinov
- Realizácia: supravodič, ión, fotón...

02 | QUBIT — MATEMATICKÝ POPIS

Stav qubit

Qubit je kvantový systém s dvoma bázovými stavmi: $|0\rangle$ a $|1\rangle$

Všeobecný stav: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

α a β sú komplexné čísla (amplitúdy pravdepodobnosti)

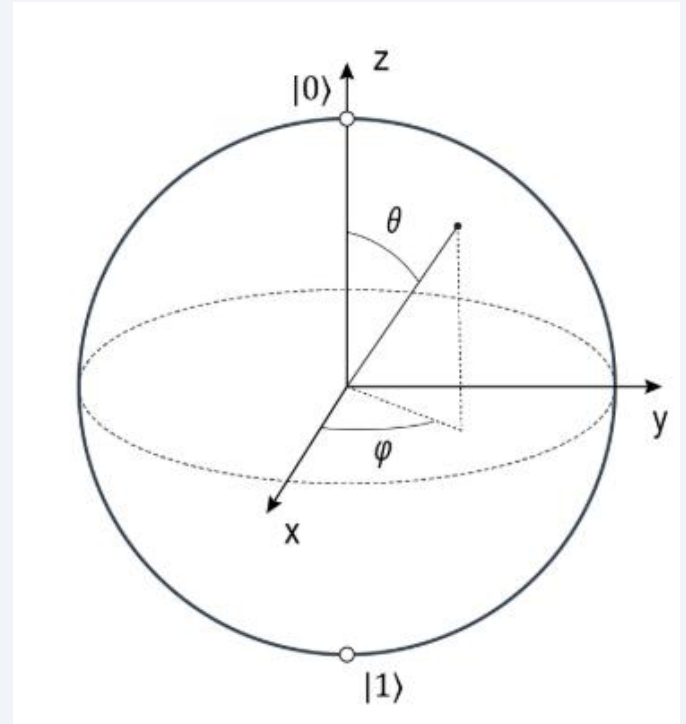
Podmienka normalizácie: $|\alpha|^2 + |\beta|^2 = 1$

Keď qubit zmeráme, dostaneme výsledok:

0 s pravdepodobnosťou $|\alpha|^2$

1 s pravdepodobnosťou $|\beta|^2$

Po meraní je stav 'zrútený' — stratíme superpozíciu!



Blochova sféra — vizualizácia ľubovoľného stavu qubit

03

Kvantové jazyky

Tri piliere kvantového výpočtu

03 | SUPERPOZÍCIA

Klasický bit

0

alebo

1



Qubit (superpozícia)

0

1

zároveň!

Čo je superpozícia?

Qubit môže byť v kombinácii stavu 0 aj 1 súčasne — kým ho nezmeráme.

Analógia

Minca letí vzduchom — je nanejsť zároveň znak aj hlava. Dopadom (meraním) sa rozhodne.

Prínos

n qubitov spracuje 2^n stavov naraz → exponenciálny paralelizmus vs klasické sekvenčné výpočty.

Pozor!

Superpozícia je krehká. Akákoľvek interakcia s okolím ju zničí (dekoherencia).

03 | PREVIAZANOSŤ (QUANTUM ENTANGLEMENT)

"Strašidelné pôsobenie na diaľku" — Albert Einstein



Čo to je?

Dva qubity sú previazané, meranie jedného okamžite určí stav druhého — bez ohľadu na vzdialenosť.

Využitie

Kvantová kryptografia (QKD), kvantová teleportácia informácie, kvantové siete.

Šírenie informácie

Previazanosť neumožňuje posielanie informácie rýchlejšie ako je rýchlosť svetla — len koreláciu.

Tretí pilier kvantového výpočtu

Interferencia umožňuje kvantovým algoritmom zosilniť správne riešenia (amplitudy) a potlačiť nesprávne — podobne ako vlny vo fyzike: konštruktívna interferencia zosilňuje, deštruktívna ruší.



správna cesta zosilnená

▲ Konštruktívna

Pravdepodobnosť správneho výsledku sa zvyšuje

▼ Deštruktívna

Pravdepodobnosť nesprávnych výsledkov klesá na nulu

nesprávna cesta zrušená

🌀 Efekt v praxi

Algoritmus 'naviguje' ku správnej odpovedi s vysokou pravdepodobnosťou

04

Ako funguje kvantový počítač?

Hradlá, obvody, meranie výsledku

04 | KVANTOVÉ HRADLÁ

Kvantové hradlá = unitárne (reverzibilné) transformácie stavov qubitov

H (Hadamard)

Uvrhne qubit do superpozície.
 $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$
Kľúčové pre väčšinu algoritmov.

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

CNOT (Riadené NOT)

2-qubitové hradlo. Ak riadiaci = $|1\rangle$, prehodí cieľový qubit.
Základné hradlo pre previazanie.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

X (Pauli-X)

Kvantový NOT — 'prehodí' qubit.
 $|0\rangle \rightarrow |1\rangle$ a $|1\rangle \rightarrow |0\rangle$
Analog klasického NOT hradla.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

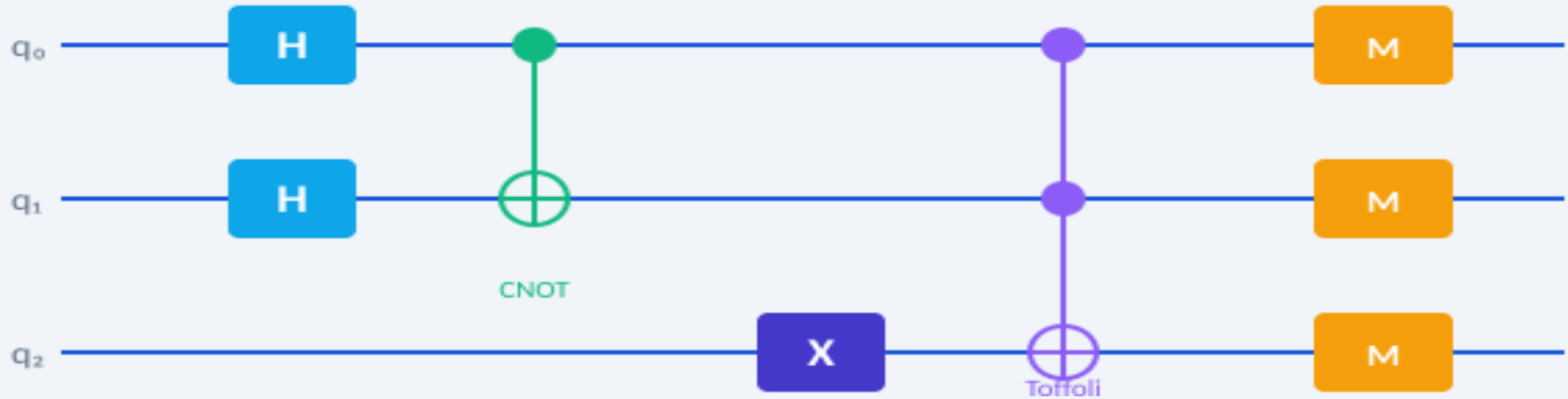
Toffoli (CCNOT)

3-qubitové hradlo. Prehodí cieľový qubit ak oba riadiace = $|1\rangle$.
Univerzálne kvantové hradlo.

$$\text{CCX (8x8 matic)} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

04 | KVANTOVÝ OBVOD A MERANIE

Kvantový obvod je postupnosť hradieľ aplikovaných na qubity — analogicky ako logické obvody v klasike.



1 Inicializácia

Qubity sa nastavujú do počiatočného stavu (zvyčajne $|0\rangle$)

2 Aplikácia hradieľ

Postupnosť kvantových operácií transformuje stav systému

3 Meranie (M)

Qubit sa zmeria — superpozícia sa zrúti na 0 alebo 1

4 Výsledok

Opakovaním získame pravdepodobnostné rozdelenie → správna odpoveď

05

Fyzická realizácia

Ako postaviť kvantový počítač v reálnom svete?

05 | TECHNOLOGIE REALIZÁCIE QUBITOV

Rôzne fyzikálne systémy môžu realizovať qubit — každý s výhodami aj nevýhodami:

Supravodivé obvody <i>IBM, Google, Rigetti</i>	✓ Rýchle hradlá ($\sim$ ns), škálovateľné, dobre preskúmané	✗ Potrebuje $\sim$ 15 mK, citlivé na šum, krátka koherencia ($\sim$ 100 μ s)
Iónové pasce <i>IonQ, Quantinuum</i>	✓ Vysoká presnosť, dlhá koherencia (minúty), nízka chybovosť	✗ Pomalšie operácie ($\sim$ μ s), ťažšia škálovateľnosť
Fotónové qubity <i>PsiQuantum, Xanadu</i>	✓ Izbová teplota, nízky šum, vhodné pre komunikáciu	✗ Náročná produkcia a detekcia fotónov, straty v optike
Topologické qubity <i>Microsoft</i>	✓ Teoreticky veľmi odolné na chyby	✗ Stále väčšinou experimentálne
NV centrá v diamante <i>Mnohé akademické lab.</i>	✓ Funguje pri izbovej teplote, dlhá koherencia	✗ Obtiažna škálovateľnosť, malý počet qubitov

Najväčší nepriateľ kvantového počítača



Čo je dekoherencia?

Qubity sú extrémne citlivé na akékoľvek vonkajšie rušenie — teplo, vibrácie, elektromagnetické polia. Interakciou s prostredím stratia kvantový charakter. Superpozícia zanikne — informácia je stratená.



Kvantová oprava chýb (QEC)

Riešenie: zakódovanie 1 logického qubitu do 50–1 000 fyzických qubitov (napr. Surface Code). Systém detekuje a opravuje chyby bez toho, aby zrušil superpozíciu.



Koherenčný čas

Typický čas počas ktorého qubit zostáva použiteľný. Supravodivé qubity: $\sim 100 \mu\text{s}$. Iónové pasce: minúty. Celý výpočet musí prebehnúť v tomto okne.



NISQ éra — kde sme dnes?

Noisy Intermediate-Scale Quantum: 100–1 000 fyzických qubitov, bez plnej korekcie chýb. Funguje pre obmedzené algoritmy s malou hĺbkou obvodu.

06

Klasický vs. Kvantový PC

Komplexné porovnanie — kedy ktorý?

06 | POROVNANIE — KLASICKÝ vs. KVANTOVÝ POČÍTAČ

Vlastnosť	 Klasický počítač	 Kvantový počítač
Základná jednotka	Bit (0 alebo 1)	Qubit (0, 1, superpozícia)
Paralelizmus	Sekvenčné/vláknó	2^n stavov súčasne
Operačná teplota	Izbová teplota	~15 millikelvinov
Chybovosť	$< 10^{-15}$ (mimoriadne nízka)	~0.1–1% (stále vysoká)
Oprava chýb	Jednoduchá parita	Komplexné kódy (Surface Code)
Vhodné pre	Word, video, web, databázy, AI	Faktorizácia, optimalizácia, simulácia
Programovanie	Python, C++, Java...	Qiskit, Cirq, Q#...
Komerčná dostupnosť	Bežne dostupné	Cloudové, vedecké laboratória

06 | KEDY POUŽIŤ KLASICKÝ A KEDY KVANTOVÝ?



Klasický počítač je lepší pre:

- Textové spracovanie, web, e-mail
- Streaming videa, herné aplikácie
- Databázové operácie (CRUD)
- Väčšinu problémov ML/AI dnes
- Finančné účtovníctvo, ERP systémy
- Operačné systémy, správa súborov
- Reálne nasadenie bez kryogeniky



Kvantový počítač je lepší pre:

- Faktorizácia obrovských čísel (kryptografia)
- Simulácia kvantovomechanických systémov
- Optimalizačné problémy (logistika, portfolio)
- Objavovanie liekov — molekulárne simulácie
- Strojové učenie s kvantovým zrýchlením
- Vyhľadávanie v databázach (Grover VN)
- Riešenie lineárnych systémov (HHL)

07

Kvantové algoritmy

Shor, Grover, VQE a iné prelomy

07 | KLÚČOVÉ KVANTOVÉ ALGORITMY

Shorov algoritmus

1994

Faktorizácia čísel

Klasický: exponenciálny čas

Kvantový: polynomiálny $O((\log N)^3)$

→ *Zlomí RSA šifrovanie!*

Groverov algoritmus

1996

Vyhľadávanie v databáze

Klasický: $O(N)$

Kvantový: $O(\sqrt{N})$

→ *Kvadratické zrýchlenie pre hľadanie.*

Kv. Fourierova transform.

1994

Základ algoritmov

Exp. rýchlejšia ako FFT.

$O(2^n) \rightarrow O(n^2)$ — exp. zrýchlenie

→ *Základ Shora, QPE a iných.*

VQE / QAOA

2014+

Hybridné kvantovo-klasické

Variačný kvantový eigenriešiteľ.

Optimalizácia na NISQ zariadeniach.

→ *Chemické simulácie, portfóliá.*

HHL algoritmus

2009

Lineárne rovnice

Systém $Ax=b$.

Exp. zrýchlenie vs gaussovka.

→ *Strojové učenie, simulácie.*

QRAM / kvantové ML

2023+

Kvantové strojové učenie

Tréning neurónových sietí.

Sledujeme potenciálne zrýchlenie.

→ *Stále aktívny výskum.*

Prečo je Shorov algoritmus tak dôležitý?

1

Problém

Faktorizácia čísla N na prvočinitele. Napr. $15 = 3 \times 5$. Pre veľké čísla (2048-bitové) trvá klasickému počítaču miliardy rokov.

2

Kvantová časť

Nájdenie periódy funkcie $f(x) = a^x \bmod N$ pomocou Kvantovej Fourierovej Transformácie.

3

Klasická časť

Z nájdenej periódy sa odvodí prvočiniteľ pomocou klasickej matematiky (GCD).

4

Výsledok

RSA-2048 faktorizovaný v hodinách/dňoch namiesto miliardy rokov!



Bezpečnostný dopad

RSA šifrovanie (internet banking, HTTPS) bude zlomiteľné

Súčasný certifikáty X.509 nebudú bezpečné

Dôverná dáta zbierané dnes môžu byť dešifrované budúci kv. počítačom

NIST 2024: nové post-quantové štandardy (CRYSTALS-Kyber, Dilithium)

Prechod na PQC kryptografiu musí začať UŽ TERAZ

08

Aplikácie

Kde kvantové počítače zmenia svet?

08 | REÁLNE APLIKÁCIE KVANTOVÝCH POČÍTAČOV

Farmácia & Medicína



Simulácia molekúl, návrh liekov, proteínové záhyby. Príklad: simulácia FeMoco (nitrogenáza) na IBM Q.

Financie & Bankovníctvo



Portfolio optimalizácia, pricing derivátov, risk analýza. JP Morgan, Goldman Sachs testujú dnes.

Kryptografia & Bezpečnosť



QKD (kvantová distribúcia kľúčov), post-quantové šifrovanie. Čínsky satelit Micius (QKD 2017).

Logistika & Optimalizácia



Problém obchodného cestujúceho, smerovanie v sieťach, letové rozvrhy — Volkswagen, DHL pilotné projekty.

Energetika



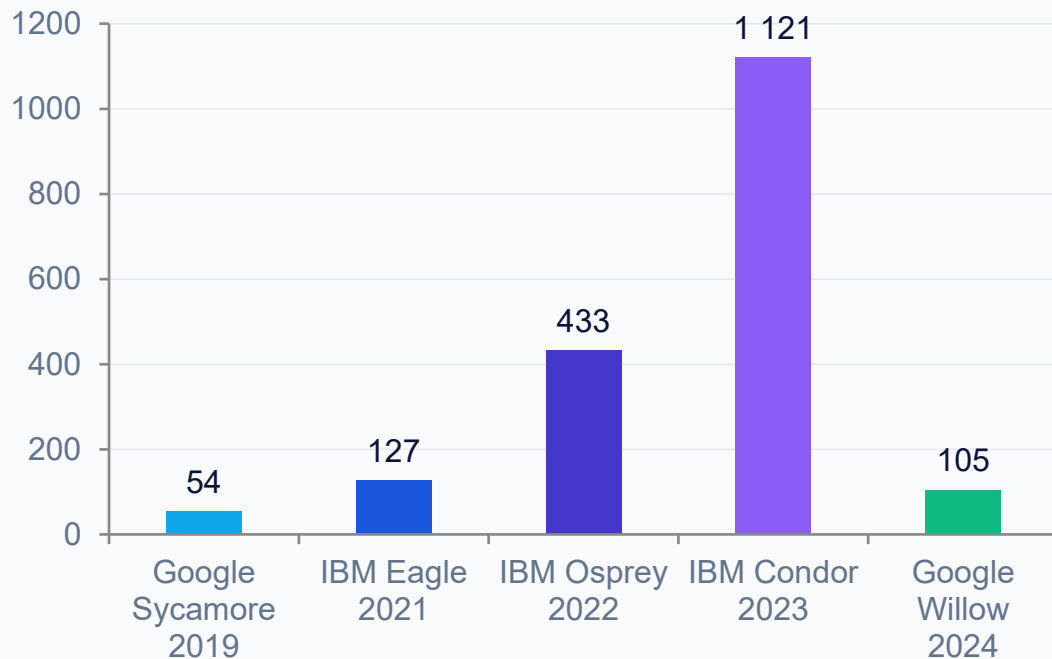
Optimalizácia sietí, batériový výskum, supravodivé materiály pre energetiku budúcnosti.

Umelá inteligencia



Kvantové strojové učenie (QML), zrýchlenie tréningovania modelov, kvantové neurónové siete.

Počet fyzických qubitov v top procesoroch



Google Sycamore 2019

54 qubitov. Úloha za 200s, superpočítač by potreboval 10 000 rokov. Prvá 'kvantová nadvláda'.

IBM Condor 2023

1 121 fyzických qubitov — rekord. Ale počet qubitov $\neq$ výkon! Dôležitá je aj kvalita (chybovosť).

Google Willow 2024

'Len' 105 qubitov, ale rekordná presnosť a oprava chýb. Výpočet za 5 min, ktorý by klasike trval 10^{25} rokov!

Záver

Závod nie je len o počte qubitov, ale o ich kvalite, konektivite a oprave chýb — to je skutočný pokrok.

09

Riziká & Výzvy

Čo stojí v ceste kvantovej revolúcii?

01 Škálovateľnosť

Každý ďalší qubit zvyšuje chybovosť celého systému. Potrebujeme 1 000–10 000 fyzických qubitov na jeden logický. IBM cieľuje na milión fyzických qubitov do 2030.

02 Dekoherencia

Kvantový stav trvá len mikrosekundy. Každý výpočet musí prebehnúť rýchlejšie ako qubit 'zabudne' svoj stav. Teplo, vibrácie, elektromagnetické polia — všetko škodí.

03 Kryogénna infraštruktúra

15 milikelvinov = chladnejšie ako hlboký vesmír (2.7 K). Každý kvantový počítač potrebuje obrovský dlučný chladič. Drahé, ťažké a nepraktické pre bežné nasadenie.

04 Programovanie & Debugging

Nové paradigma myslenia — unitárne transformácie, pravdepodobnosti. Ladenie je extrémne ťažké (meranie zničí stav). Nástroje (Qiskit, Cirq, Q#) sú ešte mladé.

05 Overenie výsledkov

Ako overíme výsledok kvantového počítača, keď nemáme iný kvantový počítač na porovnanie? A klasický je príliš pomalý pre veľké inštancie.

06 Obchodná viabilita

Zatiaľ nie je jasné, ktoré konkrétne problémy prinesú dostatočnú obchodnú hodnotu. 'Quantum hype' vs. reálna pridaná hodnota.

09 | BEZPEČNOSTNÉ RIZIKÁ & POST-KVANTOVÁ KRYPTOGRAFIA

"Harvest now, decrypt later" — útočníci dnes zbierajú šifrované dáta a čakajú na kvantový počítač.

Hrozba

- RSA a ECC (základ HTTPS, TLS) sú zraniteľné voči Shorovmu algoritmu
- VPN, digitálne podpisy, certifikáty — všetko ohrozené
- Vládne, vojenské a medicínske dáta zbierané DNES
- Kvantový počítač s ~4000 logickými qubitmi zlomí RSA-2048

Riešenie: Post-quantová kryptografia

- NIST 2024 PQC štandardy: CRYSTALS-Kyber (KEM), Dilithium (podpisy)
- FALCON, SPHINCS+ — záložné algoritmy
- Lattice-based, hash-based kryptografia — odolné voči kvantu
- Organizácie musia migrovať UŽ DNES (plánovanie trvá roky)

NIST PQC štandardy 2024 (FIPS 203 / 204 / 205):

Algoritmus	Typ	Základ	Poznámka
CRYSTALS-Kyber	Key Encapsulation	Lattice	Hlavný štandard — výmena kľúčov
CRYSTALS-Dilithium	Digitálny podpis	Lattice	Odporúčaný pre väčšinu aplikácií
FALCON	Digitálny podpis	NTRU Lattice	Kompaktné podpisy
SPHINCS+	Digitálny podpis	Hash-based	Konzervatívna voľba

09 | ETICKÉ A SPOLOČENSKÉ RIZIKÁ



Kybernetická bezpečnosť

Štáty s kvantovými počítačmi môžu dešifrovať komunikáciu iných krajín. Asymetria moci — kto má QC prvý, má obrovskú výhodu.



Energetické nároky

Kryogénne systémy sú energeticky náročné. S rastúcim počtom QC môže narásť uhlíková stopa — paradox pre 'zelenú technológiu'.



Nerovnosť prístupu

Kvantové počítače sú drahé a dostupné len veľkým korporáciám a vládny inštitúciám. Riziko technologickej priepasti medzi bohatými a chudobnými krajinami.



Regulácia a dohľad

Kto reguluje, čo sa smie robiť s kvantovými počítačmi? Export-kontroly (USA: ITAR). Hrozba zneužitia pre masové sledovanie.



Geopolitické napätie

USA, Čína, EÚ investujú miliardy do kvantovej nadradenosti. Kvantová supremácia = strategická vojenská výhoda.



Dôvera verejnosti

Ak kvantové PC zlomia šifrovanie, môže to podkopať dôveru v digitálne platby, zdravotné záznamy a demokratické procesy.

10

Budúcnosť

Roadmap a čo nás čaká v nasledujúcich desaťročiach

10 | KVANTOVÝ ROADMAP — FÁZY VÝVOJA



10 | KVANTOVÉ PC V PRAXI — PRÍSTUP DNES

Kvantové počítače sú dnes dostupné cez cloud — môžeš ich vyskúšať ZADARMO!

IBM Quantum

quantum.ibm.com

Najväčšia verejná platforma. 100+ qubitové procesory. Qiskit framework (Python). Zadarmo do určitých limitov.

Amazon Braket

aws.amazon.com

Agregátor — prístup k IonQ, Rigetti, OQC cez AWS. Platené podľa použitia. Vhodné pre firmy.

Google Quantum AI

quantumai.google

Cirq framework, Sycamore a Willow procesory. Prístup cez Google Cloud. Vhodné pre výskumníkov.

IonQ Cloud

cloud.ionq.com

Iónové pasce, vysoká presnosť. API prístup. Vhodné pre algoritmy vyžadujúce nízku chybovosť.

10 | AKO SA NAUČIŤ KVANTOVÉ PROGRAMOVANIE?

Kvantové programovanie je dostupné pre každého — potrebuješ Python a zvedavosť.

1. Základy

- Lineárna algebra (vektory, matice, unitárne transformácie)
- Komplexné čísla a pravdepodobnosť
- Základy kvantovej mechaniky (nie je potrebná fyzika VŠ)
- Python na úrovni začiatočníka

2. Prvé kroky

- Qiskit (IBM) — najlepšia dokumentácia, obrovská komunita
- IBM Quantum Learning (zadarmo, kurzy, tutoriály)
- Kniha: Nielsen & Chuang 'Quantum Computation'
- Cirq (Google), PennyLane (Xanadu) — alternatívy

3. Prax

- Spusti prvý kvantový obvod na reálnom hardware (IBM Q)
- Implementuj Groverov algoritmus (skvelý 1. projekt)
- Kaggle / Qiskit Global Summer School hackathony
- GitHub: open-source kvantové projekty

ZHRNUTIE — ČOMU SME SA DNES NAUČILI



Qubit a kvantové javy

Superpozícia, previazanosť a interferencia sú fyzikálnym základom výkonu kvantových počítačov.



Klasický vs. Kvantový PC

Nie sú konkurenti, ale doplnky. Kvantový je lepší len pre špecifické triedy problémov.



Algoritmy menia pravidlá hry

Shor faktorizuje za polynomiálny čas, Grover hľadá $\sqrt{N}$ krát rýchlejšie ako klasika.



Bezpečnostná hrozba je reálna

RSA bude zraniteľný — migrácia na post-quantovú kryptografiu (NIST 2024) je nutná UŽ DNES.



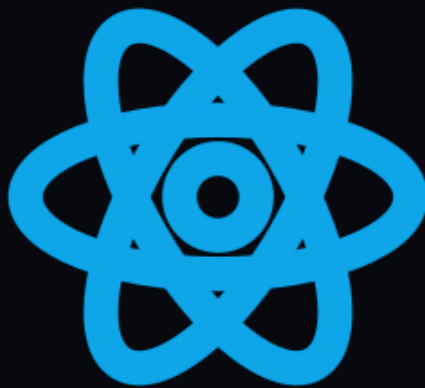
Aplikácie v reálnom svete

Medicína, financie, logistika, AI — kvantové počítače menia odvetvia v nasledujúcich 10 rokoch.



Výzvy a riziká

Dekoherencia, škálovateľnosť, etika, geopolitika — cesta k plne funkčnému QC je ešte dlhá.



Ďakujem za pozornosť!

Kvantové počítače — nie je to len sci-fi.
Je to súčasnosť a blízka budúcnosť, ktorá zmení svet.