

P R
O S T
O R

Michio Kaku

Kvantová revoluce

**Jak kvantové počítače
změní svět**

Digitální počítače nikdy nemůžou přesně spočítat, jak se atomy spojují při vzniku zásadně důležitých chemických reakcí, zejména reakcí, které umožňují život. Mohou totiž počítat jenom na digitální pásce, sestávající z řad nul a jedniček, jež jsou příliš hrubé, než aby mohly popsat jemné vlnění elektronů tančících hluboko uvnitř molekul. Když například digitální počítač zdlouhavě vypočítává pohyb myši v bludišti, musí namáhavě analyzovat všechny možné dráhy jednu po druhé. Zato kvantový počítač rychlostí blesku analyzuje všechny *najednou*.

**P R
O S T
O R**

**P R
O S T
O R**

Michio Kaku

P R
O S T
O R

Michio
Kaku

Kvantová revoluce

Jak kvantové počítače
změní svět

přeložil Jan Petříček

PRAHA | 2024

© Michio Kaku 2021
Translation © Jan Petříček 2024
Czech edition © PROSTOR 2024
ISBN 978-80-7260-592-7

Mé milující ženě Shizue a mým dcerám
dr. Michelle Kakuové a Alyson Kakuové

Obsah

Část I

Vzestup kvantových počítačů	13
1. Konec křemíkového věku	15
2. Konec digitálního věku	38
3. Vzestup kvantové teorie	54
4. Vznik kvantových počítačů	77
5. Závod začíná	107

Část II

Kvantové počítače a společnost	119
6. Původ života	121
7. Zbarvit svět dozelena	137
8. Nakrmit planetu	148
9. Dodat světu energii	160

Část III

Kvantová medicína	171
10. Kvantové zdraví	173
11. Editace genů a léčba rakoviny	187
12. Umělá inteligence a kvantové počítače	207
13. Nesmrtelnost	231

Část IV

Modelování světa a vesmíru	255
14. Globální oteplování	257
15. Slunce v láhvi	272
16. Simulace vesmíru	289
17. Jeden den v roce 2050	315

Epilog. Kvantové hádanky	325
Poděkování	339
Poznámky k jednotlivým stranám	341
Vybraná literatura	349
Autorská práva k ilustracím	351
Rejstřík	353

Část I

Vzestup kvantových počítačů

Kapitola 1

Konec křemíkového věku

Přichází revoluce.

V letech 2019 a 2020 otřásly světem vědy dvě senzační zprávy. Dvě skupiny oznámily, že dosáhly „kvantové nadvlády“ (*quantum supremacy*), bájného bodu, v němž zcela nový typ počítače, takzvaný kvantový, v určitých úlohách jednoznačně předčí běžný digitální superpočítač. Tento úspěch je předzvěstí převratu, jenž může proměnit celý svět výpočetních technologií a obrátit naruby všechny aspekty našeho každodenního života.

Nejprve společnost Google ohlásila, že její kvantový počítač Sycamore dokáže za 200 sekund vyřešit matematickou úlohu, na niž by nejrychlejší superpočítač světa potřeboval 10 000 let. V časopise *MIT Technology Review* to představitelé Googlu prohlásili za zásadní průlom. Přirovnali to

k vypuštění družice Sputnik a prvnímu letu bratří Wrightů. Stojíme prý „na prahu nové éry, éry strojů, vedle nichž budou dnešní nejvýkonnější počítače vypadat jako počítaďla“.

Institut kvantových inovací při Čínské akademii věd poté zašel ještě dál. Čínští vědci uvedli, že jejich kvantový počítač je 100bilionkrát rychlejší než běžný superpočítač.

Viceprezident společnosti IBM Bob Sutor v souvislosti s raketovým vzestupem kvantových počítačů bez okolků prohlásil: „Domnívám se, že půjde o nejdůležitější výpočetní technologii tohoto století.“

Kvantovému počítači se někdy přezdívá „počítač všech počítačů“, neboť představuje obrovský technologický pokrok s dalekosáhlými důsledky pro celý svět. Namísto na tranzistorech počítá přímo na nejmenších objektech ve vesmíru, na samotných atomech, a tak může snadno dosáhnout vyššího výkonu než naše největší superpočítače. Kvantové počítače by mohly nastolit úplně novou éru v ekonomice, společnosti a našem způsobu života.

Jsou přitom něčím víc než jen dalšími výkonnými počítači. Jsou to počítače zcela nového typu a dokážou si poradit s problémy, které by digitální počítače nikdy vyřešit nedokázaly, ani kdyby na to měly neomezeně času. Digitální počítače například nikdy nemůžou přesně spočítat, jak se atomy spojují při vzniku zásadně důležitých chemických reakcí, zejména reakcí, které umožňují život. Mohou totiž počítat jenom na digitální pásce, sestávající z řad nul a jedniček, jež jsou příliš hrubé, než aby mohly popsat jemné vlnění elektronů tančících hluboko uvnitř molekul. Když například digitální počítač zdlouhavě vypočítává pohyb myši v bludišti, musí namáhavě analyzovat všechny možné dráhy jednu po druhé. Zato kvantový počítač rychlostí blesku analyzuje všechny *najednou*.

Tento vývoj ještě zesílil vypjatou rivalitu mezi konkurenčními počítačovými giganty, kteří soupeří v tom, kdo sestrojí

nejvýkonnější kvantový počítač na světě. V roce 2021 se dostala do vedení firma IBM, když představila kvantový počítač jménem Eagle, jenž má vyšší výpočetní výkon než všechny dřívější modely.

Všechny tyto rekordy jsou však od toho, aby se překonávaly.

Vzhledem k závažným důsledkům kvantové revoluce nás nepřekvapí, že největší světové korporace investují do této nové technologie nemalé finanční prostředky. Firmy Google, Microsoft, Intel, IBM, Rigetti i Honeywell budují vlastní prototypy kvantových počítačů. Lídři Silicon Valley si uvědomují, že musejí s touto revolucí držet krok, pokud nechtějí zmizet v propadlišti dějin.

Ve snaze navnadit zvědavou veřejnost umístily společnosti IBM, Honeywell a Rigetti Computing své kvantové počítače první generace na internet, aby si je lidé mohli poprvé přímo vyzkoušet. Můžeme se tedy přes internet připojit ke kvantovému počítači a zažít kvantovou revoluci na vlastní kůži. Například platforma „IBM Q Experience“, zprovozněná v roce 2016, veřejnosti zadarmo zpřístupňuje patnáct kvantových počítačů. Mezi jejich uživatele patří firmy Samsung a JPMorgan Chase. Už nyní je každý měsíc používá 2000 lidí, od školáků po profesory.

O tuto technologii se živě zajímá i Wall Street. Jako první významná firma v oboru kvantových výpočtů vstoupila v roce 2021 na burzu společnost IonQ – a při první veřejné nabídce akcií vybrala celých 600 milionů dolarů. To však ještě nebylo to nejpřekvapivější. Konkurenční boj je tak prudký, že hodnota nového startupu PsiQuantum, jenž na trhu nemá žádný komerční prototyp a nemůže se pochlubit ani žádnými úspěchy z dřívějšíka, okamžitě vylétla na 3,1 miliardy dolarů. Skoro přes noc firma získala od investorů 665 milionů dolarů. To bylo podle obchodních analytiků něco skoro nevídaného; jen zřídkakdy se nová společnost vyvezla na

vlně horečnaté spekulace a senzacechtivých titulků do takových výšin.

Konzultantská a účetní firma Deloitte odhaduje, že trh s kvantovými počítači dosáhne stovek milionů dolarů ještě v této dekádě a desítek miliard v dekádě následující. Nikdo přesně neví, kdy kvantové počítače vstoupí na komerční trh a přetvoří ekonomickou krajinu, avšak odhady jsou neustále upravovány tak, aby odpovídaly překotnému tempu vědeckých objevů v této oblasti. Christopher Savoie, ředitel firmy Zapata Computing okomentoval úspěšné tažení kvantových počítačů slovy: „Otázka už nezní zda, ale kdy.“

Dokonce i Kongres Spojených států projevil silný zájem o to, aby urychlil příchod této nové technologie. Američtí politici si uvědomili, že jiné země už výzkum v oboru štědře financují, a v prosinci 2018 schválili zákon o národní kvantové iniciativě, jenž má poskytnout startovní kapitál k zahájení nového výzkumu. Tento zákon nařizuje založení dvou až pěti národních středisek pro výzkum kvantové informační vědy, která budou ročně dostávat 80 milionů dolarů.

V roce 2021 americká vláda oznámila další 625milionovou investici, na niž má dohlížet ministerstvo energetiky. Dalšími 340 miliony do tohoto projektu přispěly obři korporace jako Microsoft, IBM nebo Lockheed Martin.

Čína a USA nejsou jediné země, které vynakládají státní finance na urychlení vývoje této technologie. Britská vláda v současnosti staví Národní středisko pro kvantové výpočty, budoucí centrum pro výzkum kvantových výpočetních technologií, jež bude sídlit v laboratoři Harwell při Radě pro vědu a technologie v Oxfordshiru. Na popud vlády bylo ve Velké Británii do konce roku 2019 založeno třicet startupů zabývajících se kvantovými počítači.

Experti na výpočetní technologie uznávají, že jde o bilionovou sázku do loterie. V této oblasti panuje silná konkurence a nejsou tu žádné záruky. Navzdory působivým technickým

úspěchům, které si v posledních letech připsal Google a další společnosti, si na funkční kvantový počítač schopný řešit reálné problémy ještě budeme muset pár let počkat. Ještě je před námi spousta práce. Někteří kritici dokonce tvrdí, že by to mohla být honba za fatou morgánou. Počítačové společnosti si nicméně uvědomují, že kdyby dál nečinně přihlížely, mohl by jim ujet vlak.

Ivan Ostojic, partner konzultantské firmy McKinsey, tvrdí: „Firmy působící v odvětvích, v nichž mohou kvantové počítače s největší pravděpodobností způsobit naprostý převrat, by se o tyto technologie měly začít zajímat právě teď.“ V oblastech jako chemie, lékařství, ropný a plynárenský průmysl, doprava, logistika, bankovníctví, farmacie nebo kyberbezpečnost se schyluje k zásadním změnám. Ostojic dodává: „Kvantové počítače budou v zásadě relevantní pro všechny ředitele IT, neboť urychlí vývoj řešení širokého spektra problémů. Tyto společnosti si budou muset obstarat vlastní kvantové technologie.“

Vern Brownell, bývalý výkonný ředitel D-Wave Systems, kanadské společnosti věnující se kvantovým výpočtům, poznamenává: „Jsme přesvědčeni, že už velmi brzy budeme schopni vyvinout nástroje, které vám klasické počítače neposkytnou.“

Mnozí vědci se domnívají, že právě vstupujeme do zcela nové éry a že tato revoluce bude mít stejně dalekosáhlé důsledky jako vynález tranzistoru a mikročipu. Už nyní do této nové technologie investují společnosti bez přímé vazby na výrobu počítačů, například automobilový gigant Daimler, jenž vlastní Mercedes-Benz. Tuší totiž, že kvantové počítače by mohly otevřít cestu k inovacím v jejich vlastních odvětvích. Jak napsal Julius Marcea, manažer konkurenční společnosti BMW: „Zkoumání potenciálu kvantových technologií transformovat automobilový průmysl nás naplňuje nadšením a jsme odhodláni posouvat hranice technických možností.“

Jiné velké společnosti, jako Volkswagen nebo Airbus, zřídily vlastní oddělení výzkumu kvantových výpočtů, aby zjistily, jak tyto novinky promění jejich podnikání.

Vývoj v tomto oboru pozorně sledují i farmaceutické společnosti. Uvědomují si, že kvantové počítače možná budou schopny simulovat složité chemické a biologické procesy, které dalece překračují schopnosti počítačů digitálních. Rozsáhle střediska, kde se dnes testují miliony léků, snad jednoho dne nahradí „virtuální laboratoře“, které je budou testovat v kyberprostoru. Objevují se obavy, že tyto počítače připraví o práci chemiky. Derek Lowe, autor blogu o farmaceutickém výzkumu, však tvrdí: „Nejde o to, že stroje nahradí chemiky. Ve skutečnosti jenom chemikové používající stroje nahradí ty, kteří je nepoužívají.“

Kvantové technologie dnes používá dokonce i Velký hadronový urychlovač u Ženevy ve Švýcarsku, největší vědecký přístroj na světě, v němž se vědci snaží napodobit podmínky panující v počátcích vesmíru tím, že vyvolávají srážky protonů s energií 14 bilionů elektronvoltů. Kvantové počítače jim pomáhají s pročesáváním obrovských hromad dat. Za jedinou sekundu zvládnou analyzovat až jeden bilion bytů generovaných asi miliardou srážek částic. Jednoho dne tedy kvantové počítače možná rozluští tajemství vzniku vesmíru.

Kvantová nadvláda

Když fyzik John Preskill z Kalifornského technologického institutu v roce 2012 přišel s termínem „kvantová nadvláda“, mnozí vědci jenom kroutili hlavou. Měli za to, že to bude trvat desetiletí, ne-li staletí, než kvantové počítače budou schopny překonat své digitální konkurenty. Provádění výpočtů

na jednotlivých atomech namísto na křemíkových čípech se pokládalo za pekelně komplikovanou záležitost. Křehký tanec atomů v kvantovém počítači může narušit sebemenší vibrace nebo šum. Ohromující zprávy o dosažení kvantové nadvlády nicméně zatím chmurné předpovědi škarohlídů vyvracejí. Obavy se nyní týkají naopak toho, jak překotně se obor vyvíjí.

Zemětřesení vyvolané těmito pozoruhodnými úspěchy způsobilo otřesy i v zasedacích místnostech korporací a sídlech zpravodajských služeb po celém světě. Dokumenty zveřejněné whistleblowery ukázaly, že CIA a Národní bezpečnostní agentura (NSA) vývoj v oboru pečlivě monitorují. Kvantové počítače jsou totiž tak výkonné, že by v principu mohly rozluštit všechny známé šifrovací kódy. To znamená, že by se žárlivě strážena tajemství vlád – jejich nejcennější poklady obsahující nejcitlivější informace – mohla ocitnout v ohrožení. Totéž platí i pro nejprísněji utajovaná tajemství korporací nebo i jednotlivců. Situace je natolik naléhavá, že dokonce i americký Národní institut standardů a technologie (NIST), který má na starosti státní technologickou politiku a standardy, vydal směrnice, jež mají velkým korporacím a agenturám pomoci s přípravou na nevyhnutelný přechod do této nové éry. NIST očekává, že do roku 2029 budou kvantové počítače schopny prolomit 128bitové AES šifrování, používané mnoha společnostmi.

Ali El Kaafarani v časopise *Forbes* podotýká: „To je pořádně děsivá vyhlídka pro každou organizaci, která potřebuje chránit nějaká citlivá data.“

Číňané do své Národní laboratoře pro kvantové informační vědy investovali 10 miliard dolarů, protože jsou odhodláni stát se v tomto klíčovém a dynamicky se rozvíjejícím oboru lídry. Státy utrácí desítky miliard, aby své šifry ochránily. Lze si představit, že hacker vyzbrojený kvantovým počítačem by se mohl vládat do *jakéhokoli* digitálního počítače na planetě a potenciálně tak narušit fungování celých průmyslových

odvětví nebo i armád. Všechny citlivé informace se možná dostanou do rukou toho, kdo za ně nabídne nejvíc. Kdyby kvantové počítače pronikly do útrob Wall Streetu, mohl by rozvrat zachvátit i finanční trhy. Nadto by hackeři mohli odemknout blockchain a napáchat tak spoušť také na trhu s bitcoiny. Společnost Deloitte odhaduje, že hackerský útok provedený kvantovým počítačem by mohl ohrozit asi 25 procent těchto elektronických peněz.

„Ti, kdo provozují blockchainové projekty, budou nejspíš pokroky kvantových výpočtů sledovat se značnou nervozitou,“ uzavírá zpráva IT společnosti CB Insights, zabývající se datovým softwarem.

V sázce tedy není nic menšího než sama globální ekonomika, která je dnes těsně provázána s digitálními technologiemi. Banky na Wall Streetu používají počítače ke sledování mnohamiliardových transakcí. Inženýři pomocí nich navrhují mrakodrapy, mosty nebo rakety. Umělci by bez nich nemohli vytvořit animované kasovní trháky. Farmaceutické společnosti je používají k vývoji nových zázračných léků. Děti na nich se svými kamarády hrají nejnovější videohry. A navíc nutně potřebujeme mobilní telefony, abychom mohli být neustále v kontaktu s přáteli, spolupracovníky a příbuznými. Všech se nás někdy zmocnila panika, když jsme nemohli najít mobil. Vlastně by bylo nesmírně obtížné jmenovat nějakou lidskou činnost, kterou počítače nepřevrátily vzhůru nohama. Jsme na nich tak závislí, že kdyby všechny počítače světa najednou z nějakého důvodu přestaly fungovat, uvrhlo by to civilizaci do chaosu. Proto vědci sledují vývoj kvantových počítačů s tak živým zájmem.

Konec Moorova zákona

Co je příčinou všeho toho rozruchu a všech těch sporů?

Vzestup kvantových počítačů je známkou toho, že se pomalu, ale jistě chýlí ke konci křemíkový věk. V posledním půlstoletí se prudký růst výpočetního výkonu řídil Moorovým zákonem, pojmenovaným podle zakladatele firmy Intel Gordona Moora. Moorův zákon tvrdí, že se výpočetní výkon zdvojnásobuje každých osmnáct měsíců. Tento zdánlivě prostý zákon předpověděl pozoruhodný exponenciální růst výpočetního výkonu, jaký nemá v lidských dějinách obdoby. Neexistuje žádný jiný vynález, jenž by za tak krátkou dobu měl podobně dalekosáhlé dopady.

Počítače v průběhu dějin prošly mnoha fázemi, přičemž každá z nich přinesla mnohonásobné zvýšení jejich výkonu a vyvolala převratné společenské změny. Ve skutečnosti lze platnost Moorova zákona rozšířit až do 19. století, období mechanických počítačů. Tehdy konstruktéři používali k provádění jednoduchých aritmetických operací rotující válce, převody a ozubená kola. Na začátku 20. století začaly tyto kalkulačky používat elektřinu; převody nahradila relé a kabely. Během druhé světové války počítače luštily tajné vládní šifry pomocí ohromného množství elektronek. V poválečném období se přešlo od elektronek k tranzistorům, které lze miniaturizovat na mikroskopickou velikost, což usnadnilo další pokroky v rychlosti a výkonu.

V padesátých letech 20. století se používaly sálové počítače, které si mohly dovolit jenom velké korporace, nadnárodní banky a vládní agentury jako Pentagon. Ty sice byly výkonné (například počítač ENIAC zvládl za třicet vteřin to, co by člověku trvalo dvacet hodin), jenže byly také drahé a rozměrné; často zabíraly celé jedno patro kancelářské budovy. Mikročip vnesl do celého procesu revoluci. Postupem času se zmenšoval do té míry, že typický čip o velikosti nehtu nyní

dokáže obsáhnout asi miliardu tranzistorů. Mobily, na nichž dnes děti hrají videohry, jsou výkonnější než celá místnost plná těch těžkopádných dinosaurů, které kdysi používal Pentagon. Už nám ani nepříjde nic zvláštního na tom, že počítač v naší kapse svým výkonem předčí počítače používané během studené války.

Všechno jednou pomine. Vývoj počítačů byl procesem tvořivé destrukce, při němž při každém přechodu na vyšší stupeň dřívější technologie zastarala. Moorův zákon již nyní začíná zpomalovat a možná se nakonec zastaví. Mikročipy jsou totiž tak malinké, že nejtenčí vrstva tranzistorů má šířku jen zhruba dvacet atomů. Když toto číslo klesne na pět, stává se poloha elektronů neurčitou; elektrony pak mohou prosakovat ven a způsobovat zkraty anebo generovat tolik tepla, že se čip roztaví. Jinými slovy, jestliže budeme dál používat primárně křemík, Moorův zákon se podle zákonů fyziky musí nakonec zhroutit. Možná jsme právě svědky konce křemíkového věku. Další skok by nás mohl přenést do věku postkřemíkového či kvantového.

Jak to vyjádřil Sanjay Natarajan ze společnosti Intel: „Domníváme se, že z téhle architektury už víc vymáčkнуть nejde.“

Ze Silicon Valley by se jednoho dne mohl stát další „Rezavý pás“.

Ačkoli nyní zdánlivě panuje klid, tato budoucnost dříve nebo později přijde. Jak tvrdí Hartmut Neven, ředitel AI laboratoře Googlu: „Vždycky to vypadá, že se pořád nic neděje, nic se neděje – a najednou šup, a jste v úplně jiném světě.“

Proč jsou tak výkonné?

Proč jsou kvantové počítače tak výkonné, že se státy celého světa předhánějí v tom, kdo tuto novou technologii ovládne jako první?

V podstatě všechny moderní počítače jsou založeny na digitálních informacích, které lze zakódovat do posloupností nul a jedniček. Nejmenší jednotka informace, jediná číslice, se jmenuje bit. Tato řada nul a jedniček je vložena do digitálního procesoru, který provede výpočet a pak nám dá výsledek. Například rychlost vašeho internetového připojení lze měřit jednotkou bity za sekundu (bps), což znamená, že každou sekundu je do vašeho počítače posílána miliarda bitů. Díky tomu získáváte okamžitý přístup k filmům, e-mailům, dokumentům atd.

Laureát Nobelovy ceny Richard Feynman nicméně roku 1959 vytušil možnost jiného přístupu k digitálním informacím. V prorocké, průlomové eseji „There’s Plenty of Room at the Bottom“ (Tam dole je spousta místa) a v pozdějších článkách si položil otázku: Proč místo posloupností nul a jedniček nepoužít stavy atomů a nesestrojit tak atomový počítač? Proč nenahradit tranzistory nejmenším možným objektem, atomem?

Atomy jsou jako roztočené dětské káči. V magnetickém poli mohou být vzhledem k tomuto poli orientovány buď nahoru, nebo dolů, což může odpovídat nule nebo jedničce. Výkon digitálního počítače závisí na počtu stavů (nul či jedniček), které ve svém počítači máte.

Díky prapodivným pravidlům subatomárního světa se však atomy mohou také nacházet v jakékoli kombinaci obou těchto stavů. Například můžete mít stav, v němž rotační osa (neboli spin) atomu 10 % času míří nahoru a 90 % času dolů. Anebo 65 % času míří nahoru a 35 % času dolů. Ve skutečnosti existuje nekonečně mnoho způsobů, jak se atom může otáčet.

To ohromně zvyšuje množství možných stavů. Atom tak může obsáhnout daleko více informací – ty už nejsou uloženy v bitu, ale v qubitu (kvantovém bitu), tj. směsi stavů „nahoru“ i „dolů“. Digitální bity mohou najednou nést jenom jeden bit informací, což omezuje jejich výkon. Zato výkon qubitů – kvantových bitů – je takřka neomezený. Skutečnost, že na atomární úrovni mohou objekty existovat v několika stavech najednou, se nazývá superpozice. (To rovněž znamená, že na atomární úrovni jsou běžně porušovány dobře známé zákony zdravého rozumu. V tomto měřítku mohou být elektrony na dvou místech současně, což pro velké předměty neplatí.)

Kromě toho tyto qubity mohou na rozdíl od běžných bitů interagovat jeden s druhým. Tomu se říká „provázání“ (*entanglement*). Zatímco stavy digitálních bitů jsou vzájemně nezávislé, bude každý další qubit, který do počítače přidáte, interagovat se všemi stávajícími, čímž se počet možných interakcí zdvojnásobí. Kvantové počítače jsou tedy ze své podstaty exponenciálně výkonnější než počítače digitální, neboť množství interakcí zdvojnásobíte pokaždé, když připojíte další qubit.

Dnes například kvantové počítače mohou mít přes 100 qubitů. To znamená, že jsou 2^{100} krát výkonnější než superpočítač s pouhým jedním qubitem.

Kvantový počítač Sycamore společnosti Google, který jako první dosáhl kvantové nadvlády, dokáže se svými třiapadesáti qubity zpracovat 72 trilionů bytů paměti (trilion je miliarda miliard). Svým výkonem tedy zcela zastihuje jakýkoli běžný počítač.

To má obrovský význam pro vědu i ekonomiku. Jak se přesouváme od digitální ke kvantové světové ekonomice, je toho v sázce neobyčejně mnoho.

Překážky na cestě ke kvantovým počítačům

Další klíčová otázka zní: Proč si nemůžeme už nyní v obchodě koupit kvantový počítač? Proč nějaký podnikavý vynálezce nepředstaví kvantový počítač, který bude umět rozluštit jakoukoli známou šifru?

Když Richard Feynman poprvé navrhl koncept kvantového počítače, předjímal i problém, jemuž bude čelit. Aby kvantové počítače fungovaly, musejí být atomy uspořádány tak, aby kmitaly přesně unisono. Tomu se říká „koherence“. Jenže atomy jsou neuvěřitelně maličké a citlivé. Seběmenší nečistota nebo rušivý vliv z vnějšího světa mohou způsobit, že se koherence souboru atomů rozpadne, což celý výpočet pokazí. Tato křehkost je hlavním problémem, s nímž se kvantové počítače potýkají. Otázka za miliardu tedy zní: Dokážeme zkrotit dekoherenci?

K omezení kontaminace zvnějšku používají vědci zvláštní vybavení, jež snižuje teplotu skoro až na absolutní nulu. Při takto nízkých teplotách je nechtěných vibrací jen minimálně, ale k jejich dosažení potřebujeme speciální a nákladné pumpy a trubice.

Stojíme však před jednou záhadou. Matka příroda bez obtíží používá kvantovou mechaniku i při pokojové teplotě. Například zázrak fotosyntézy, jeden z nejdůležitějších dějů na Zemi, je kvantový proces, který se nicméně odehrává při normálních teplotách. Matka příroda nepotřebuje k uskutečnění fotosyntézy místnost plnou exotických přístrojů pracujících při teplotách blízkých absolutní nule. Z důvodů, jimž příliš nerozumíme, zůstává v přírodě koherence zachována i za teplého slunečného dne, přestože by rušivé vlivy z vnějšího světa měly na atomární úrovni vyvolávat chaos. Kdybychom jednoho dne pochopili, jak matka příroda provádí svá kouzla při pokojové teplotě, mohli bychom se stát pány kvanta, ba i života samotného.

Revoluce v ekonomice

Ač kvantové počítače v krátkodobém horizontu představují hrozbu pro kyberbezpečnost, v dlouhodobém horizontu mají velký praktický potenciál. Mohly by vnést revoluci do světové ekonomiky, stvořit udržitelnější budoucnost a zahájit éru kvantové medicíny, která by pomohla vyléčit dříve nevléčitelné nemoci.

Existuje mnoho oblastí, v nichž kvantové počítače mohou překonat ty běžné digitální.

1. Vyhledávače

V minulosti se bohatství měřilo ropou nebo zlatem.

Dnes se stále častěji měří množstvím dat. Zatímco dříve společnosti svá finanční data vyhazovaly, nyní si uvědomují, že tyto informace jsou cennější než vzácné kovy. Běžný digitální počítač však na prohledávání této záplavy dat nemusí stačit. A tady vstupují do hry kvantové počítače, jež by mohly najít příslovečnou jehlu v kupce sena. Budou možná schopny analyzovat finanční situaci společnosti a vyhmátnout hrstku faktorů, které jí brání v růstu.

Banka JPMorgan Chase skutečně nedávno uzavřela partnerství s firmami IBM a Honeywell, které jí mají pomoci analyzovat její data, lépe předpovídat finanční rizika a nejistotu a zefektivnit její fungování.

2. Optimalizace

Až kvantové počítače pomocí vyhledávačů najdou v datech klíčové faktory, další otázkou bude, jak je upravit, aby se maximálně zvýšila hodnota určitých parametrů, například zisku. Velké korporace, univerzity a vládní agentury budou kvantové počítače využívat přinejmenším k tomu, aby minimalizovaly náklady a maximalizovaly efektivitu a zisk. Čistý zisk společnosti závisí na stovkách činitelů, jako jsou mzdy,

prodeje, výdaje atd., a ty všechny se v průběhu času rychle mění. Úkol najít správnou kombinaci faktorů, která zvýší zisk firmy, je pro tradiční digitální počítač nezvládnutelný. Finanční společnosti zase možná budou kvantové počítače používat k předpovídání budoucího vývoje finančních trhů, na nichž se každý den odehrávají transakce o hodnotě miliard dolarů. Těmto firmám tedy kvantové počítače poskytnou výpočetní výkon nezbytný k optimalizaci jejich hospodářských výsledků.

3. Simulace

Kvantové počítače by dále mohly řešit složité rovnice, jež překračují schopnosti digitálních počítačů. Strojírenským firmám možná pomůžou vypočítat aerodynamické vlastnosti tryskáčů, letounů a automobilů a najít ideální tvar, který by snižoval tření, minimalizoval náklady a maximalizoval efektivitu. Vlády by je mohly využívat k předpovídání počasí – například aby zjistily dráhu ničivého hurikánu nebo vypočítaly, jakým způsobem změna klimatu za desítky let ovlivní naši ekonomiku a způsob života. A vědci by mohli pomocí kvantových počítačů pátrat po ideální konfiguraci magnetů v obřích jaderných fúzních reaktorech, která by jim umožnila ovládnout moc vodíkové fúze a „chytit Slunce do láhve“.

Snad vůbec nejpřínosnějším využitím kvantových počítačů však bude simulace stovek zásadně důležitých chemických dějů. Ideální by bylo, kdybychom bez jakýchkoli chemikálií, jenom s kvantovými počítači dokázali předpovědět výsledek libovolné chemické reakce na atomární úrovni. Tento nový vědecký obor, výpočetní chemie, nezjišťuje chemické vlastnosti experimentálně, nýbrž tak, že je simuluje na kvantovém počítači. Tento postup by mohl jednoho dne nahradit nákladné a zdlouhavé testování. Z celé biologie, medicíny i chemie by se stala kvantová mechanika. To by obnášelo vytvoření „virtuální laboratoře“, kde bychom mohli v paměti kvantového

počítače rychle zkoušet nové léky, terapie a léčebné postupy. Obešli bychom se tak bez desetiletí pokusů a omylů i bez pomalých a úmorných laboratorních experimentů. Místo abychom prováděli tisíce složitých, nákladných a časově náročných chemických pokusů, mohli bychom jednoduše stisknout tlačítko kvantového počítače.

4. Spojení AI a kvantových počítačů

Umělá inteligence (AI) se umí výtečně učit ze svých chyb, a tak postupně zvládat čím dál náročnější úkoly. Již se osvědčila v průmyslu i lékařství. Jedno z jejích omezení ovšem tkví v tom, že ohromné množství dat, jež musí zpracovávat, může snadno přehltnout běžný digitální počítač. Schopnost prohledávat hromady dat je naopak jednou ze silných stránek kvantových počítačů. Spolupráce obou technologií tak může výrazně zlepšit jejich schopnost řešit problémy všeho druhu.

Další uplatnění kvantových počítačů

Kvantové počítače mají moc přetvořit celá průmyslová odvětví. Kupříkladu by mohly konečně nastolit dlouho očekávaný věk slunce. Futurologové a vizionáři už celá desetiletí předpovídají, že obnovitelná energie vytlačí fosilní paliva a vyřeší skleníkový efekt, který způsobuje oteplování naší planety. Celé zástupy těchto snů a myslitelů vychvalují přednosti obnovitelné energie.

Jenomže věk slunce pořád ne a ne přijít.

I když cena větrných turbín a solárních panelů poklesla, pořád představují jenom zlomek celosvětové výroby energie. Čím to je?

Žádná nová technologie si nemůže dovolit ignorovat to nejdůležitější: náklady. Po několika desetiletích, kdy opěvovali sluneční a větrnou energii, si jejich zastánci musejí přiznat, že obnovitelná energie je v průměru pořád dražší než fosilní paliva. Důvod je zřejmý. Když slunce nesvítí a vítr nefouká, zařízení na výrobu obnovitelné energie leží ladem a sedá na ně prach.

Nástupu věku slunce brání jeden klíčový faktor, který se často přehlíží. Jsou jím baterie. Jsme zhýčkaní tím, že výpočetní výkon roste exponenciální rychlostí, a nevědomky předpokládáme, že se tímtež tempem zlepšují všechny elektronické technologie.

Raketový růst výpočetního výkonu je zčásti způsoben tím, že při vyleptávání maličkých tranzistorů do křemíkového čipu můžeme používat stále kratší vlnové délky ultrafialového záření. Jenže baterie jsou jiný, zapeklitější případ; pracují se směsí exotických chemikálií ve složité vzájemné souhře. Energie baterií roste jenom pomalu a namáhavě, metodou pokusu a omylu, nikoli systematickým zkracováním vlnové délky UV světla. A navíc je energie uložená v baterii pouhým zlomkem energie uložené v benzínu.

To by kvantové počítače mohly změnit. Snad budou schopny modelovat tisíce možných chemických reakcí, abychom mohli i bez jejich provádění v laboratoři zjistit, která z nich bude nejefektivnější pro výrobu superbaterie, a tak věk slunce konečně nastolit.

Již nyní se automobilky a dodavatelé energií snaží vyřešit problém skladování energie s využitím kvantových počítačů první generace od firmy IBM. Pokoušejí se zvýšit kapacitu a rychlost nabíjení příští generace lithium-sírových baterií. Tím se však možný dopad kvantových počítačů na klima nevyčerpává. Společnost ExxonMobil se navíc s pomocí kvantových počítačů od IBM pokouší stvořit nové chemikálie, které by se daly využít k energeticky úspornému zpracovávání

surovin a zachytávání oxidu uhličitého. Zejména si od kvantových počítačů slibuje, že budou schopny simulovat různé materiály a zjistit jejich chemické vlastnosti, například tepelnou kapacitu.

Zakladatel firmy PsiQuantum Jeremy O'Brien zdůrazňuje, že v této revoluci nejde o budování rychlejších počítačů, nýbrž o řešení problémů – třeba složitých chemických a biologických reakcí –, které by žádný běžný počítač nikdy vyřešit nedokázal, byť bychom mu na to dali sebevíc času.

O'Brien tvrdí: „Nemluvíme o tom, že budeme některé věci dělat rychleji nebo lépe ..., ale o tom, že je vůbec budeme schopni dělat. ... Tyto problémy budou vždy mimo dosah jakéhokoli běžného počítače, který sestrojíme... I kdybychom vzali všechny atomy křemíku na planetě a vyrobili z nich superpočítač, pořád bychom tyto ... obtížné problémy nedokázali vyřešit.“

Nakrmit planetu

Dalším významným uplatněním kvantových počítačů by mohlo být nakrmení rozrůstající se světové populace. Některé bakterie dokážou bez námahy vzít ze vzduchu dusík a vytvořit z něj amoniak, jenž se následně přeměňuje v chemické látky sloužící jako hnojiva. Tento proces fixace dusíku je důvodem, proč na zemi vzkvétá život; umožňuje růst bujné vegetace, která krmí lidi i zvířata. Když se chemikům podařilo tento kousek napodobit Haberovým-Boschovým procesem, přineslo to takzvanou zelenou revoluci. Tento proces nicméně vyžaduje obrovské množství energie. Ve skutečnosti se na něj vynakládají ohromující dvě procenta celosvětové produkce energie.

To je kuriózní paradox. *Bakterie zadarmo dělají něco, co spotřebovává značnou část světové energie.*

Otázka zní: Mohou kvantové počítače vyřešit tento problém efektivní výroby hnojiva a zahájit druhou zelenou revoluci? Někteří futurologové předpovídají, že bez další revoluce ve výrobě potravin může nastat ekologická pohroma. Nakrmit stále rostoucí světovou populaci bude čím dál obtížnější, což by mohlo vést k masovému hladovění a rozpoutat hladové bouře po celé planetě.

Vědci z Microsoftu už učinili první pokusy o využití kvantových počítačů ke zvýšení účinnosti hnojiv a odhalení tajemství fixace dusíku. V budoucnu by kvantové počítače mohly zachránit lidskou civilizaci před ní samotnou. Dalším zázrakem přírody je fotosyntéza, při níž se sluneční světlo a oxid uhličitý přeměňují v kyslík a glukózu, které pak tvoří základ skoro veškerého živočišného života. Bez fotosyntézy by se potravní řetězec zhroutil a život na naší planetě by brzy uchřádl.

Vědci tráví už desítky let tím, že se snaží rozkrýt všechny kroky tohoto procesu, molekulu po molekule. Jenomže přeměna světla v cukr je kvantově mechanický děj. Po letech úsilí badatelé identifikovali body, v nichž tomuto procesu vévodí kvantové jevy – a všechny jsou mimo dosah digitálních počítačů. Proto se ani našim nejlepším chemikům dosud nedaří vytvořit umělou fotosyntézu, která by mohla být účinnější než ta přírodní.

Je možné, že kvantové počítače budou s to vynalézt efektivnější umělou fotosyntézu anebo úplně nové způsoby, jak zachytit energii slunečního světla. A to možná rozhodne o tom, zda bude mít lidstvo v budoucnu co jíst.

Zrod kvantové medicíny

Kvantové počítače tedy možná omladí životní prostředí a rostlinnou říši. Zároveň však mohou vyléčit nemocné a umírající. Nejenže dokážou rychleji než jakýkoli běžný počítač analyzovat účinnost milionů potenciálních léků současně, navíc mohou objasnit samotnou povahu nemoci.

Kvantové počítače by mohly zodpovědět otázky jako: Co způsobuje náhlou změnu zdravých buněk v buňky nádorové a jak by se jejich bujení dalo zastavit? Co zapříčiňuje Alzheimerovu chorobu? Proč jsou Parkinsonova nemoc a amyotrofická laterální skleróza (ALS) nevyléčitelné? Anebo příklad z nedávné doby: Víme, že koronavirus mutuje – ale jak nebezpečné všechny tyto varianty jsou a jak budou reagovat na léčbu?

Mezi největší objevy v dějinách medicíny patří antibiotika a vakcíny. Jenomže nová antibiotika objevujeme víceméně metodou pokusu a omylu, aniž přesně chápeme, jak fungují na molekulární úrovni, a vakcíny jenom podněcují lidské tělo k vytvoření látek, jimiž se bude útočícímu viru bránit. V obou případech zůstávají konkrétní molekulární mechanismy záhadou – a kvantové počítače nás možná poučí o tom, jak bychom mohli vyvinout lepší vakcíny a antibiotika.

První obrovský krok k pochopení lidského organismu učinil Projekt lidského genomu, když sestavil soupis všech 3 miliard párů bází a 20 000 genů, které tvoří konstrukční plán našeho těla. Ale to je jenom začátek. Problém je v tom, že digitální počítače, používané hlavně k prohledávání rozsáhlých databází známých genetických kódů, nám nijak nepomůžou s objasněním toho, jak přesně DNA a proteiny konají v těle své zázraky. Proteiny (neboli bílkoviny) jsou složité látky, které sestávají často až z tisíců atomů a při provádění svých molekulárních kouzel se specifickými a nevysvětlitelnými způsoby sbalují do malých kuliček. Na nejzákladnější úrovni má

veškerý život kvantově mechanickou povahu, takže je mimo dosah digitálních počítačů.

S kvantovými počítači však pokročíme do další fáze, v níž rozluštíme mechanismy na molekulární úrovni, které nám řeknou, jak tyto procesy fungují. To vědcům dovolí vyvinout nové genetické dráhy, léky a terapie a vyléčit dosud nevyléčitelné nemoci.

Farmaceutické společnosti jako ProteinQure, Digital Health 150, Merck nebo Biogen už zakládají výzkumná centra, která budou zkoumat, jak kvantové počítače ovlivní analýzu léčiv.

Vědci nevycházejí z údivu nad tím, že matka příroda dokázala stvořit nepřeberné množství molekulárních mechanismů, které umožňují zázrak života. Tyto mechanismy jsou nicméně jen vedlejším produktem náhody a přírodního výběru probíhajícího už miliardy let. Proto pořád trpíme některými nevyléčitelnými nemocemi a neduhy stáří. Jakmile pochopíme, jak tyto molekulární mechanismy fungují, budeme je moci s využitím kvantových počítačů vylepšit nebo vyvinout jejich nové verze.

Genomika například dokáže s pomocí počítačů identifikovat geny jako BRCA1 nebo BRCA2, jejichž mutace mohou vést ke vzniku rakoviny prsu. Digitální počítače nám však nijak nepomůžou se zjištěním toho, jak přesně tyto poškozené geny rakovinu způsobují. A také ji nedokážou zastavit, jakmile se rozšíří po celém těle. Kvantové počítače by naopak mohly rozluštit molekulární záludnosti našeho imunitního systému, a tak nám pomoci vyvinout nové léky a léčebné postupy k boji s těmito nemocemi.

Dalším příkladem je Alzheimerova choroba, o níž se někteří lidé domnívají, že vzhledem k stárnutí populace bude „nemocí století“. Digitální počítače nám mohou ukázat, že s touto chorobou souvisejí mutace v některých genech, jako je gen ApoE4. Neumějí však vysvětlit, proč tomu tak je.

Podle jedné z hlavních teorií způsobují Alzheimerovu chorobu priony, amyloidové proteiny, které se v mozku svinují nesprávně. Když odbojná molekula vrazí do molekuly jiné bílkoviny, způsobí, že se nesprávně sbalí i ona. Nemoc se tedy může šířit kontaktem, přestože v ní nehrají roli bakterie ani viry. Panuje podezření, že vzpurné priony by mohly být viníky alzheimerera, parkinsona, ALS a řady dalších nevléčitelných nemocí postihujících seniory.

Problém skládání proteinů je tedy jedním z nejdůležitějších nezmapovaných území biologie. Ve skutečnosti může ukrývat tajemství života samotného. Otázka, jak přesně se nějaká proteinová molekula sbaluje, však překračuje schopnosti všech běžných počítačů. Zato kvantové počítače by mohly odhalit nové cesty, jak odbojné bílkoviny zneškodnit a vyvinout nové léčebné postupy.

Dále by se mohlo ukázat, že budoucností medicíny bude výše zmiňované spojení AI a kvantových počítačů. AI programy jako AlphaFold už nyní dokázaly zmapovat detailní atomární strukturu ohromujících 350 000 typů proteinů, včetně všech proteinů, z nichž se skládá lidské tělo. Dalším krokem je použít jedinečné metody kvantových počítačů ke zjištění toho, jak tyto bílkoviny dělají svá kouzla, a k vynalezení nové generace léků a terapií.

Již nyní dochází k propojování kvantových počítačů s neuronovými sítěmi. Cílem je vytvořit novou generaci učících se strojů, které se budou doslova samy přebudovávat. Oproti tomu laptop na vašem stole se nikdy neučí. Dnes není o nic výkonnější než vloni. Až poslední dobou si počítače díky novým pokrokům v hlubokém učení začínají uvědomovat své chyby a učit se. Kvantové počítače by mohly tento proces exponenciálně urychlit a zásadně ovlivnit lékařství i biologii.

Výkonný ředitel Googlu Sundar Pichai přirovnává příchod kvantových počítačů k přelomovému prvnímú letu bratří Wrightů z roku 1903. Původní pokus nebyl sám o sobě nijak