KAPITOLA TŘINÁCTÁ

FYZIKÁLNÍ POVAHA INFORMACE

Před „tím" byl bit

Čím více energie, tím rychleji se mění bity. Zemi, vzduch, oheň i vodu tvoří energie, ale různé podoby, kterých nabývají, jsou určovány informací. K jakékoli činnosti potřebujeme energii. Ke specifikaci činnosti potřebujeme informaci.[1]

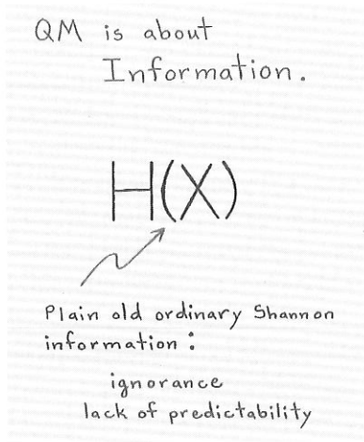
SETH LLOYD (2006)

Za svou krátkou historii přestála kvantová mechanika více krizí, sporů, interpretací (kodaňskou, Bohmovu, mnohasvětovou, dekoherenční...), výbušného dělení na frakce a filozofických exkurzů než jakákoli jiná věda. Je prostoupena tajemstvím a vesele přehlíží lidskou intuici. Albert Einstein zemřel nesmířený s jejími důsledky a Richard Feynman nevtipkoval, když řekl, že ji nikdo nechápe. Dohady o povaze reality se asi dají očekávat - kvantová fyzika, která je tak záhadně úspěšná v praxi, se teoreticky zabývá základy všeho a její vlastní základy se neustále přestavují. I tak se ale zdá, že vření je spíše náboženské než vědecké.

Christopher Fuchs, který pracoval jako kvantový teoretik v Bell Labs a později v kanadském ústavu Perimeter Institute, se ptá: „Jak k tomu došlo?"[2]

> Navštivte jakékoli setkání a budete si připadat jako ve svatém městě v době velkého svátku. Najdete tam všechna náboženství s jejich kněžími zabředlá do svaté války - bohmisty, zastánce konzistentní historie, transakcionalismu, spontánního kolapsu, výběru vyvolaného prostředím, kontextuálního objektivismu, naprosté everettisty a mnoho dalších. Všichni prohlašují, že vidí světlo konečné pravdy. A všichni nám tvrdí, že když přijmeme jejich řešení jako svého spasitele, uvidíme světlo i my.

Fuchs říká, že je čas začít znovu. Odmrštit existující kvantové axiomy s jejich vytříbeným matematickým stylem a uchýlit se k hlubším fyzikálním principům: „Tyto principy by měly být jiskrné a působivé. Měly by oslovit duši." A kde je lze nalézt? Fuchs si na svou otázku sám odpovídá: v kvantové teorii *informace:* „Důvod je jednoduchý a myslím nevyhnutelný. Kvantová mechanika se vždy týkala informace - společenství fyziků na to pouze zapomnělo."[3]



Vizuální pomůcka od Christophera Fuchse.
(V kvantové mechanice jde o informaci. Stará obyčejná Shannonova informace: nevědomost, nepředvídatelnost.)

Jedním z těch, kteří nezapomněli (nebo si znovu vzpomněli), byl John Archibald Wheeler - průkopník jaderného štěpení, Bohrův student a Feynmanův učitel, autor termínu „černá díra" a poslední velikán fyziky 20. století. Liboval si v epigramech i aforismech. Když chtěl vyjádřit, že zvenčí černé díry lze pozorovat pouze hmotnost, náboj a spin, napsal slavný výrok: *Černá díra nemá vlasy.* A pokračoval: „Učí nás to, že vesmír lze zmačkat jako kus papíru až do nekonečně malého bodu, že čas je možné uhasit jako plamen a že fyzikální zákony, které považujeme za ‚posvátné' a neměnné, jsou vším ostatním, jen ne právě tím."[4] V roce 1989 nabídl svůj poslední chytlavý obrat: *Před „tím" byl bit* [It from bit]. Jeho hledisko bylo krajní. „To" bylo nehmotné - nejprve zde byla informace, všechno ostatní přišlo až později. Prohlásil:

> Jinak řečeno, každé „to" - každá částice, každé silové pole, i samo časoprostorové kontinuum - odvozuje svou úlohu, smysl, samotnou existenci... z *bitů.*[5]

Proč se zdá příroda kvantovaná? Protože kvantovaná je informace. Bit je nejmenší nedělitelná částice.

Mezi fyzikálními jevy, které dostávaly informaci do popředí pozornosti, nebyl žádný tak velkolepý jako černé díry. Nejdřív se ovšem zdálo, že vůbec žádnou informaci neobsahují.

Černé díry jsou duchovním dítětem Alberta Einsteina, který se však nedočkal jejich skutečného objevení. V roce 1915 odvodil, že světlo podléhá gravitaci, že gravitace zakřivuje strukturu časoprostoru a že dostatečná hmotnost ve zhuštěném stavu - například hvězda - bude zvyšovat svou gravitaci a neomezeně se smršťovat, až se zcela zhroutí. Důsledky vypadají tak podivně, že trvalo téměř půl století, než se jim lidé postavili tváří v tvář. Dovnitř vchází vše, ven nevychází nic. Zvláštnost leží v samotném středu. Hustota se stává nekonečnou, gravitace rovněž, časoprostor se nekonečně zakřivuje. Čas a prostor se zamění. Žádné světlo, žádný signál nemůže uniknout ven, a proto jsou takové věci ze své podstaty neviditelné. Wheeler jim začal říkat „černé díry" v roce 1967. Astronomové jsou přesvědčeni, že některé z nich našli - vyplynuly z gravitační interference - a nikdo se nikdy nemůže dozvědět, co je v jejich nitru.

Nejprve se astrofyzici zaměřili na hmotu a energii, jež se řítí dovnitř. Později si začali dělat starosti s informací. Problém se objevil, když v roce 1974 Stephen Hawking přidal k obvyklým výpočtům obecné relativity kvantové efekty a tvrdil, že černé díry by přece jen měly vyzařovat částice - jako důsledek kvantových fluktuací poblíž horizontu událostí.[6] Jinými slovy, černé díry se pomalu vypařují. Problém spočíval v tom, že Hawkingovo záření je bez jasné formy, beztvaré. Jedná se o tepelné záření. Hmota, která se řítí *do* černé díry, však nese informaci v samotné struktuře, uspořádání, kvantových stavech - z hlediska statistické mechaniky ve svých dostupných mikrostavech. Dokud chybějící informace zůstávala mimo dosah, za horizontem událostí, fyzici si s ní nemuseli dělat starosti. Stačilo jim říci, že je nedostupná, ale neztratila se. Jak řekl v roce 1625 Francis Bacon: „Ve tmě se budou shodovat všechny barvy."

Hawkingovo záření však nenese žádnou informaci. Kam se poděje informace, až se černá díra vypaří? Podle kvantové mechaniky se informace neztrácí. Deterministické fyzikální zákony vyžadují, aby stavy fyzikálního systému v jednom okamžiku určovaly stavy v příštím okamžiku - v mikroskopických detailech se zákony dají obrátit a informace se musí zachovat. Hawking byl první, kdo rozhodně (až alarmisticky) prohlásil, že tento problém otřásá samotnými základy kvantové mechaniky. Ztráta informace by narušila unitaritu - princip, že pravděpodobnosti musí dávat součet jedna. Hawkins prohlásil: „Nejenže Bůh hraje v kostky, ale také je někdy hodí tam, kde nejsou vidět." V létě roku 1975 předložil časopisu *Physical Review* pojednání s dramatickým názvem „Selhání fyziky v gravitačním kolapsu". Časopisu trvalo přes rok, než se je (s umírněnějším názvem) vůbec odhodlal otisknout.[7]

Článek se setkal s rázným protestem jiných fyziků, jak ostatně Hawking očekával. Jedním z nich byl John Preskill z Kalifornského technického institutu. Nadále byl přesvědčen o principu, že informace se nemůže ztratit -

třebas když beze zbytku shoří kniha, ale vy dokážete vysledovat každý foton a každý kousek popela, můžete ji zase obnovit. Na semináři v Kalifornském technickém institutu Preskill varoval: „Ztráta informace je vysoce nakažlivá představa. Kvantovou teorii lze velmi těžko změnit tak, aby se smířila s ideou ztráty informace, aniž by to proniklo do všech procesů."[8] V roce 1997 uzavřel s Hawkingem velice medializovanou sázku, že informace musí z černé díry nějakým způsobem unikat. Vsadili se o encyklopedii podle vítězova výběru. Leonard Susskind ze Stanfordu, který podpořil Preskilla, řekl: „Někteří fyzici mají pocit, že otázka, co se děje v černé díře, je akademická nebo dokonce teologická. Něco jako počítání andělů na špičce jehly. Tak to ale vůbec není. Ve hře je budoucí fyzika."[9] Během několika let bylo navrženo mnoho různých řešení. Sám Hawking v jednu chvíli pronesl: „Myslím, že informace asi odchází do jiného vesmíru, matematicky jsem to ale ještě nebyl schopen předvést."[10]

Až v roce 2004 Hawking s konečnou platností přiznal, že změnil názor a že sázku prohrál. Podle svých slov již našel způsob, jak předvést, že kvantová gravitace je přece jen unitární a že informace zůstává zachována. Použil formalismus kvantové neurčitosti - „součtu přes všechny historie" Feynmanových dráhových integrálů - na samotnou topologii časoprostoru a *de facto* prohlásil, že černé díry nejsou nikdy jednoznačně černé. Napsal: „Zmatek a paradoxy nastaly proto, že lidé uvažovali typicky z hlediska jediné topologie pro časoprostor."* Někteří fyzici byli jeho novým vyjádřením zaskočeni. Připadalo jim jako mlhavé a ponechávalo mnohé otázky nezodpovězené. V jednom byl však rozhodný. Napsal: „Neodděluje se zde žádný potomek našeho vesmíru, jak jsem si kdysi myslel. Informace spolehlivě setrvává v našem vesmíru. Je mi líto, že zklamu příznivce science-fiction."[11] Preskillovi koupil encyklopedii o baseballu s názvem *Total Baseball: The Ultimate Baseball Encyclopedia*. Měla 2 688 stran, „ze kterých lze informace získat bez problémů", podotkl. A dodal: „Ale možná jsem mu z nich měl dát jen ten popel."

Charles Bennett se k teorii kvantové informace dostal úplně jinak. Dávno před tím, než rozvinul svou ideu logické hloubky, uvažoval o „termodynamice výpočtů".[12] Bylo to osobité téma, protože zpracování informace se většinou chápalo jako zbavené tělesnosti. Bennett uvedl: „Až se všichni přestanou podivovat nad termodynamikou výpočtů, nebude jako předmět vědeckého zkoumání vypadat o nic zvláštněji než například termodynamika lásky." Je to jako energie myšlení. Kalorie se mohou vydávat, ale nikdo je nepočítá.

* Bylo to buď R^4, nebo černá díra. Feynmanovo shrnutí historie však umožňuje, aby to bylo obojí najednou.

Bennett se pokoušel prozkoumat termodynamiku nejmenšího termodynamického počítače, kterým byl neexistující, abstraktní, idealizovaný Turingův stroj. Sám Turing se nikdy nezabýval tím, že by jeho myšlenkový experiment spotřebovával nějakou energii nebo vydával teplo při poslušném pohybu nahoru a dolů po fiktivních papírových páskách. Přesto začátkem 80. let 20. století Bennett hovořil o použití pásek do Turingových strojů jako paliva - jejich kalorický obsah se měl měřit v bitech. Byl to samozřejmě stále myšlenkový experiment, který se měl soustředit na reálnou otázku: Jaká je fyzická cena logické práce? Provokativně napsal: „O počítačích lze uvažovat jako o strojích, které mění volnou energii na odpadní teplo a matematickou práci."[13] Znovu se na scéně objevila entropie. Páska plná nul, páska se zakódovaným Shakespearovým dílem i páska s číslicemi π má „cenu paliva". Páska s náhodným záznamem žádnou cenu nemá.

Bennett, jehož rodiče byli učiteli hudby, vyrůstal na newyorském předměstí Westchester. V 60. letech vystudoval chemii na Brandeis University a pak studoval na Harvardu. V té době tam vyučoval James Watson, jenž přednášel o genetickém kódu, a Bennett mu rok dělal asistenta. Získal doktorát v molekulární dynamice - prováděl počítačové simulace, které přes noc běžely na stroji s pamětí asi 20 000 desítkových číslic a generovaly výstup dat na nesčetných stránkách tabelačního papíru. K pokračování svého výzkumu molekulárního pohybu potřeboval výkonnější počítače, a tak se přesunul do Lawrence Livermore Laboratory v kalifornském Berkeley, poté do Argonne National Laboratory v Illinois a nakonec se v roce 1972 přidal k výzkumu společnosti IBM.

IBM samozřejmě nevyráběla Turingovy stroje. V jednu chvíli však Bennettovi svitlo, že jeden specializovaný Turingův stroj se již nachází v přírodě: je to RNA-polymeráza, o které ho učil sám Watson. Polymeráza je enzym, který se pohybuje podél genu - což je jeho „páska" - a přepisuje DNA. Pohybuje se vlevo a vpravo, jeho logické stavy se mění podle chemické informace zapsané v sekvenci a jeho termodynamické chování se dá měřit.

Ve skutečném světě narůstala v 70. letech 20. století energetická účinnost hardwaru tisíckrát rychleji než v předchozí éře elektronek, přesto však elektronické počítače stále ztrácejí velké množství energie v podobě odpadního tepla. Čím více se blíží teoretickému minimu spotřeby energie, tím naléhavěji se vědci chtějí dozvědět, jaké vlastně to teoretické minimum je. Von Neumann, který pracoval s obřími počítači, učinil hrubý odhad již v roce 1949 - navrhl množství tepla, jež se musí rozptýlit „k provedení elementárního informačního děje, tedy elementárního výběru ze dvou možností a elementárního přenosu jedné jednotky informace".[14] Svůj odhad založil na molekulární práci

odvedené v modelovém termodynamickém systému Maxwellovým démonem podle novější formulace Leó Szilárda.* Von Neumann uvedl, že tuto cenu musí zaplatit každý elementární informační děj, každá volba ze dvou možností. V 70. letech to bylo obecně přijímáno. Ale bylo to špatně.

Von Neumannovu chybu objevil vědec, který se stal Bennettovým instruktorem v IBM - uprchlík z nacistického Německa Rolf Landauer.[15] Svou profesionální kariéru zasvětil hledání fyzikálního základu informace. „Information Is Physical" („Informace je fyzikální") byl název jednoho slavného pojednání, které mělo připomenout, že výpočetní technika si vyžaduje fyzické objekty a řídí se fyzikálními zákony. Aby na to nikdo nezapomněl, nazval pozdější esej (která byla jeho poslední) „Information Is Inevitably Physical" („Informace je nevyhnutelně fyzikální"). Trval na tom, že ať už je bitem znak na hliněné tabulce, dírka v děrném štítku nebo částice se spinem nahoru a dolů, nemůže existovat bez *nějakého* ztělesnění. V roce 1961 se Landauer pokusil dokázat von Neumannovu formuli pro náklady informačního zpracování a zjistil, že to nejde. Naopak se zdálo, že většina operací nemá z hlediska entropie vůbec žádné náklady. Když se bit překlopí z nuly na jedničku nebo obráceně, informace zůstává zachována. Proces je vratný. Entropie se nemění - žádné teplo se nemusí rozptýlit. Došel k závěru, že entropii zvyšuje pouze nevratná operace.

Landauer a Bennett byli zvláštní dvojice. Spořádaný mladý muž, typický zaměstnanec IBM - a vedle něj zanedbaný hippie (přinejmenším v Bennettových očích).[16] Mladší Bennett se zabýval Landauerovým principem a analyzoval nejrůznější druhy počítačů, skutečné i abstraktní, od Turingových strojů a mediátorové RNA po „balistické" počítače, které přenášely signály podobně jako odrážející se kulečníkové koule. Potvrdil, že velkou část výpočetního procesu lze uskutečnit bez jakýchkoli energetických nákladů. Zjistil, že k rozptylu tepla dochází pouze tehdy, když je informace *vymazána*. Vymazání je nevratná logická operace. Když hlavice Turingova stroje vymaže jedno políčko pásky nebo když elektronický počítač vybije kondenzátor, bit se ztratí, a *pak* musí dojít k rozptylu tepla. V Szilárdově myšlenkovém experimentu démon nezpůsobuje náklady entropie, když molekulu sleduje nebo vybírá. K placení dochází až ve chvíli vyčištění záznamu, kdy démon vymaže historii jednoho sledování molekuly, aby měl prostor na další.

Zapomínání vyžaduje práci.

---

* Von Neumannova formule pro teoretické energetické náklady každé logické operace byla kT ln 2 jouly za bit, když T je pracovní teplota počítače a k je Boltzmanova konstanta. Szilárd prokázal, že démon v jeho stroji může získat kT ln 2 práce z každé molekuly, kterou si vybere, takže energetické náklady se musí splatit někde v průběhu cyklu.

Bennett podotýká: „Možná řeknete, že to je pomsta teorie informace kvantové mechanice.“[17] Občas může úspěšný nápad v jednom oboru překážet pokroku v jiném. V tomto případě byl úspěšným nápadem princip neurčitosti - přináší vědomí hlavní úlohy, kterou hraje samotný proces měření. Už nelze mluvit o pouhém „sledování“ molekuly - pozorovatel musí použít fotony, ty musí mít více energie než tepelné pozadí, a následují komplikace. V kvantové mechanice má proces pozorování své vlastní důsledky, ať už se mu věnuje vědec v laboratoři nebo Maxwellův démon. Příroda je na naše experimenty citlivá.

Dále Bennett říká: „Kvantová teorie vyzařování pomohla lidem dojít k nesprávnému závěru, že výpočty mají v každém kroku termodynamické náklady, které se nedají snížit. Ve druhém případě vedl úspěch Shannonovy teorie zpracování informací k tomu, že lidé oddělili celou fyziku od zpracování informace a považovali to za výhradně matematickou záležitost.“ Když se návrháři čipů a lidé od komunikace začali přibližovat úrovni atomů, dělali si stále více starostí s tím, že do jejich klasické schopnosti jasně rozlišit mezi stavy nula a jedna začne zasahovat kvantová neurčitost. Nyní se na to však podívali znovu, a právě zde se nakonec zrodila kvantová informatika. Bennett a jeho kolegové začali uvažovat jinak. Kvantové efekty nemusí přinášet jen nepříjemnosti, naopak mohou poskytnout výhodu.

Ve výzkumné laboratoři IBM v zalesněných kopcích Westchesteru stojí u stěny Bennettovy kanceláře přístroj, který je ukrytý před světlem jako truhla s výbavou nevěsty. Pojmenovali ho Teta Marta (což byl kratší název pro „Rakev tety Marty“). Bennett a jeho výzkumný asistent John Smolin ho zhotovili v letech 1988 a 1989 s pomocí laboratorních dílen - je to hliníková skříňka zevnitř nastříkaná matnou černou barvou a utěsněná pryžovými uzávěry a černým sametem.[18] Pomocí kalibračního helium-neonového laseru a vysokonapěťových článků k polarizaci fotonů poslali tito dva vědci poprvé v historii zprávu kódovanou kvantovou kryptografií. Byla to vzorová ukázka informatické úlohy, kterou zvládne jen kvantový systém. Brzy nato následovaly kvantová oprava chyb, kvantová teleportace a kvantové počítače.

Kvantovou zprávu si vyměnili Alice a Bob - všudypřítomný smyšlený pár. Alice a Bob začali svou kariéru v kryptografii, ale nyní pracují i pro kvantový výzkum, kde se k nim občas připojí i Charlie. Stále vcházejí do různých místností, házejí mincí a posílají si zalepené obálky. Vybírají si stavy a provádějí Pauliho rotace. Barbara Terhalová, Bennettova kolegyně a jedna z teoretiček kvantové informace nové generace, vysvětluje: „Říkáme například: ‚Alice pošle Bobovi qubit a zapomene, co udělala‘, ‚Bob provede měření a výsledek sdělí Alici‘.“[19] Sama Barbara Terhalová zjišťovala, zda jsou Alice a Bob *monogamní* pár - šlo přirozeně o další technický pojem.

V experimentu s Tetou Martou posílá Alice Bobovi informaci, která je zašifrovaná, aby si ji nemohl přečíst nějaký zlomyslný třetí člověk nebo skupina lidí (často je odposlouchává nepřátelsky naladěná Eva). Když oba znají soukromý klíč, Bob dokáže zprávu rozluštit. Ale jak Alice tento klíč Bobovi pošle? Bennett spolu s informatikem Gillesem Brassardem z Montrealu začali tím, že kódovali každý bit informace jako jeden kvantový objekt, dejme tomu foton. Informace se nachází v kvantových stavech fotonu, například v horizontální nebo vertikální polarizaci. Objekt v klasické fyzice, který se skládá z miliard částic, můžeme zachytit, kontrolovat, sledovat a posílat dál, ale u kvantového objektu to možné není. Kvantový objekt nelze ani kopírovat či klonovat. Samotné sledování objektu zprávu nevyhnutelně naruší. Ať se slídilové snaží odposlouchávat jakýmkoli způsobem, jsou odhaleni. Alice se řídí složitým, velmi spletitým protokolem, který vypracovali Bennett a Brassard, a vytváří posloupnost náhodných bitů, jež se má použít jako klíč. Bob pak na druhém konci dokáže sestavit totožnou posloupnost.[20]

První experimenty s Tetou Martou dokázaly poslat kvantové bity v atmosférickém vzduchu na vzdálenost 32 centimetrů. Nebylo to žádné *Pane Watsone, přijďte sem, rád bych vás viděl* - v historii kryptografie se ovšem objevilo něco jedinečného: zcela nerozluštitelný šifrovací klíč. Později výzkumní pracovníci přešli na optické vlákno. A Bennett mezitím přešel ke kvantové teleportaci.

Tohoto názvu zalitoval velmi brzy, když marketingové oddělení IBM uvedlo jeho práci v reklamě se sloganem „Dávej pozor, budu ti teleportovat guláš.“[21] Nicméně teleportace fungovala, a tak název zůstal. Alice neposílá guláš, ale qubity.*

Qubit je nejmenší netriviální kvantový systém. Stejně jako typický bit má dvě možné hodnoty - nulu a jedničku - tedy dva stavy, které lze spolehlivě rozlišit. V klasickém systému se v zásadě dají rozlišit *všechny* stavy. (Pokud nedokážete odlišit jednu barvu od druhé, máte jen nedokonalý měřicí přístroj.) V kvantovém systému je však díky Heisenbergovu principu neurčitosti nedokonalá rozlišitelnost všude - když měříte jakoukoli vlastnost kvantového objektu, ztrácíte tím schopnost měřit komplementární vlastnost. Můžete zjistit buď hybnost, nebo polohu částice, ale nelze zjistit obojí. Mezi další komplementární

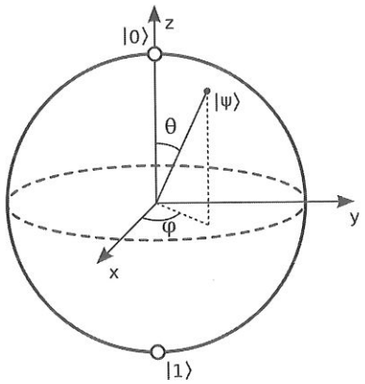
* Toto slovo není uznáváno všeobecně, třebaže slovník OED ho v prosinci 2007 přijal. Téhož roku napsal David Mermin: „Naneštěstí nyní vládne absurdní pravopis slova *qubit*... I když „qubit“ ctí anglické (německé, italské...) pravidlo, že za *q* má následovat *u*, přehlíží stejně podstatný požadavek, že za *qu* má následovat samohláska. „Qubit“ byl podle mne uznán proto, že opticky připomíná zastaralou anglickou jednotku délky, homonymický *cubit*. K pochopení jeho neobratnosti si postačí představit... že člověk zavrhl průhlednost a vyčistil si uši *quičinkami*.“ N. David Mermin, *Quantum Computer Science: An Introduction* (Cambridge: Cambridge University Press, 2007), s. 4.

vlastnosti patří směry spinu a - jako v případě Tety Marty - rovněž polarizace. Fyzici uvažují o těchto kvantových stavech geometrickým způsobem - jako o stavech systému, které odpovídají směrům v prostoru (vícerozměrném), a jejich rozlišitelnost závisí na tom, zda jsou tyto směry „ortogonální", kolmé.

Nedokonalá rozlišitelnost je právě tím, co kvantové fyzice dává jakýsi snový nádech - neschopnost sledovat systémy bez jejich narušení, neschopnost klonovat kvantové objekty nebo je vyslat několika posluchačům. Qubit má tento snový nádech také. Není to jen buď - anebo. Jeho hodnoty 0 a 1 představují kvantové stavy, které lze spolehlivě rozlišit (například horizontální a vertikální polarizace), ale současně s nimi existuje celé kontinuum mezistavů (například diagonální polarizace), jež se mohou blížit k nule nebo jedničce s různými pravděpodobnostmi. Fyzik tedy řekne, že qubit je *superpozice* stavů - kombinace amplitud pravděpodobnosti. Je to určitá věc se skrytým závojem neurčitosti. Qubit však není popleta. Superpozice není míchanice, ale kombinace pravděpodobnostních složek podle jasných a elegantních matematických pravidel.

Bennett tvrdí: „Nenáhodný celek může mít náhodné části. Je to vrcholně neintuitivní část kvantové mechaniky, nicméně vychází z principu superpozice, a pokud víme, příroda se tak chová. Lidem se to nemusí hned líbit, ale po čase si na to zvyknou; jiné možnosti jsou daleko horší."

Klíčem k teleportaci a velké části kvantové informatiky je jev zvaný entanglement, kvantové provázání. Entanglement se chopí principu superpozice a rozšíří ho v prostoru na pár qubitů, které jsou od sebe velmi vzdálené. V určitém stavu jsou jako *pár*, přestože ani jeden z nich nemá vlastní měřitelný stav. Než entanglement objevili, museli si ho vymyslet - v tomto případě to byl opět Einstein. Pak ho museli pojmenovat, což neučinil Einstein, ale Schrödinger.



Qubit

Einstein ho vymyslel pro účely myšlenkového experimentu, který měl osvětlit domnělé chyby v kvantové mechanice ve stavu z roku 1935. Spolu s Borisem Podolskym a Nathanem Rosenem experiment publikoval ve známém pojednání „Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" („Lze kvantově mechanický popis fyzické reality považovat za úplný?")[22] Pojednání se proslavilo i tím, že Wolfganga Pauliho přimělo napsat Werneru Heisenbergovi: „Einstein se znovu veřejně vyjádřil o kvantové mechanice... Dobře víme, že kdykoli to udělá, je to katastrofa."[23] Myšlenkový experiment si představoval pár částic ve zvláštním vzájemném vztahu - jako když je například pár fotonů emitován jediným atomem. Jejich polarizace je náhodná, ale stejná - v tuto chvíli i po celou dobu jejich existence.

Einstein, Podolsky a Rosen zjišťovali, co se stane, když jsou fotony od sebe velmi vzdálené a jeden z nich změříme. V případě provázaných částic - páru fotonů, který byl vytvořen společně a nyní se rozdělil na vzdálenost mnoha světelných let - se zdá, že měření jednoho fotonu má vliv i na druhý foton. V okamžiku, kdy Alice změří vertikální polarizaci svého fotonu, bude mít Bobův foton na této ose také určitý stav polarizace, zatímco jeho diagonální polarizace bude neurčitá. Měření tak vytvoří vliv, který se zjevně šíří rychleji než světlo. Vypadalo to jako paradox a Einstein k tomu cítil odpor. Napsal: „To, co skutečně existuje v místě B, by nemělo záviset na tom, jaký druh měření se provádí v místě A."[24] Své pojednání uzavřel stroze: „Od žádné rozumné definice reality se nedá očekávat, že by toto dopustila." Pojmenoval to nesmazatelnými slovy *spukhafte Fernwirkung*, „strašidelné působení na dálku".

V roce 2003 izraelský fyzik Asher Peres navrhl na hádanku trojice Einstein-Podolsky-Rosen (EPR) možnou odpověď. Nechal se slyšet, že jejich pojednání není úplně chybné, ale bylo napsáno příliš brzy, před tím, než Shannon vytvořil svoji teorii informace, „a trvalo pak ještě mnoho let, než se teorie informace stala součástí výbavy fyziků".[25] Informace má fyzikální povahu. Nemá smysl hovořit o kvantových stavech a nevzít přitom v úvahu *informaci* o kvantových stavech.

> Informace není jen abstraktní představa. Potřebuje fyzického nositele, který je (zhruba) lokalizován. Koneckonců, činností Bellovy telefonní společnosti bylo přepravovat informaci od jednoho telefonu k druhému, na jiné místo.
>
> ...Když Alice změří svůj spin, jí získaná informace zůstává tam, kde se Alice nachází - a to trvá až do okamžiku, kdy se rozhodne ji rozšířit. V místě, kde se nachází Bob, se neděje vůbec nic... Až tehdy, když se Alice rozhodne informovat Boba o získaném výsledku (e-mailem, telefonem,

rozhlasem nebo pomocí jakéhokoli jiného hmotného nosiče, který je přirozeně omezen rychlostí světla), Bob zjistí, že jeho částice má určitý čistý stav.

Christopher Fuchs ostatně tvrdí, že hovořit o kvantových stavech nemá vůbec smysl. Kvantový stav je konstrukt pozorovatele, z čehož pramení mnoho nesnází. Opusťte stavy, vstupte do informace: „Terminologie o tom může říci vše - ten, kdo se věnuje tomuto oboru a alespoň někdy přemýšlel o jeho kvantových základech, řekne ‚kvantová informace' se stejnou pravděpodobností jako ‚kvantový stav' ... ‚Co dělá protokol kvantové teleportace?' Dnes by běžná odpověď zněla: ‚Přenáší kvantovou informaci z místa, kde se nachází Alice, na místo, kde je Bob.' To, k čemu zde dochází, je změna způsobu myšlení, duševního postoje."[26]

Hádanka strašidelného působení na dálku nebyla ještě zcela rozluštěna. *Nelokalita* byla předvedena v různých důmyslných experimentech, které vyšly z myšlenkového experimentu EPR. Ukazuje se, že provázanost je nejen skutečná, ale také všudypřítomná. Pár atomů v každé molekule vodíku, H_2, je kvantově provázaný („*verschränkt*", jak řekl Schrödinger). Bennett zapojil provázanost do kvantové teleportace, která byla poprvé veřejně představena v roce 1993.[27] Teleportace používá provázaný pár k projekci kvantové informace z třetí částice na libovolnou vzdálenost. Alice nemůže tuto třetí částici změřit přímo - místo toho změří něco o jejím vztahu k jedné z provázaných částic. I když Alice sama nezná kvůli principu neurčitosti originál, Bob může obdržet přesnou kopii. Objekt Alice je v průběhu dění netělesný. Komunikace není rychlejší než světlo, protože Alice musí poslat Bobovi ještě běžnou (nekvantovou) zprávu. Bennett se svými kolegy napsal: „Výsledek teleportace je zcela prozaický - [kvantový objekt] je odebrán z rukou Alice a po přiměřené době se objeví v rukách Boba. Pozoruhodné je pouze to, že v mezidobí se informace jasně rozdělila na klasickou a neklasickou část."

Výzkumným pracovníkům rychle naskakovaly představy nejrůznějšího použití, například přenos nestálé informace do bezpečného úložiště či paměti. S gulášem i bez něho budila teleportace rozruch, protože přinášela nové možnosti, jak uskutečnit reálný, ale dosud stále prchavý sen kvantového počítání.

Idea kvantového počítače je zvláštní. Richard Feynman si tuto zvláštnost zvolil na samotném začátku, když v roce 1981 přednášel v MIT - poté, co poprvé zkoumal možnost použití kvantového systému k výpočtům obtížných kvantových problémů. Začal trochu rozpustile: „Tajemství! Tajemství! Zavřete dveře..."[28] Pak pokračoval:

Vždy jsme obtížně chápali pohled na svět, který reprezentuje kvantová mechanika. Přinejmenším já, protože jsem již dost starý, abych se dostal tak daleko, že mi to bude jasné [bylo mu 62 let]. No tak dobrá, stále mě to znervózňuje... Pořád nechápu to, že žádný skutečný problém neexistuje. Skutečný problém nedokážu definovat, a proto mám dojem, že neexistuje, ale nejsem si tím jistý.

Dobře věděl, jaký problém to byl pro výpočetní techniku - pro simulaci kvantové fyziky na počítači. Problémem byla pravděpodobnost. Každá kvantová proměnná zahrnovala pravděpodobnosti, což složitost výpočetních procesů zvyšovalo exponenciálně: „Počet informačních bitů je stejný jako počet bodů ve vesmíru, a tak byste k vyloučení pravděpodobnosti museli popsat asi N^N konfigurací, a to je na náš počítač příliš... Podle uvedených pravidel je proto nemožné provádět simulaci pomocí výpočtu pravděpodobností."

Navrhl tedy bojovat ohněm proti ohni: „Jiný způsob simulace probabilistické Přírody, kterou pro tuto chvíli nazvu *N*, může stále znamenat simulaci probabilistické Přírody počítačem *C*, který je sám probabilistický." Uvedl, že kvantový počítač nebude Turingovým strojem. Bude to něco úplně nového.

Bennett poznamenává: „Feynman to chápal tak, že kvantový systém v určitém smyslu neustále propočítává svou budoucnost. Dá se říci, že je to analogový počítač vlastní dynamiky."[29] Vědci rychle přišli na to, že kdyby měl kvantový počítač mimořádnou schopnost vypořádat se s problémy při simulaci fyziky, mohl by vyřešit i jiné problémy, které nyní nedokážou zdolat.

Tato schopnost pochází z onoho mihotavého, nehmatatelného objektu: qubitu. Pravděpodobnosti má vestavěné. Ztělesnění superpozice stavů dává qubitu větší schopnost než typickému bitu, který se vždy nachází jen v jednom nebo v druhém stavu, ve stavu 0 nebo 1 - jak říká David Mermin: „ubohý exemplář dvourozměrného vektoru."[30] Rolf Landauer suše poznamenal: „Když jsme se naučili počítat na svých ulepených klasických prstech, byli jsme uvedeni v omyl. Mysleli jsme si, že celé číslo musí mít určitou a jedinečnou hodnotu." A ono to tak není - ve skutečném, tedy kvantovém světě.

Při kvantovém počítání jsou četné qubity vzájemně provázané. Pokud je přimějeme fungovat společně, nebude se jejich výpočetní síla násobit; poroste exponenciálně. Při klasických výpočtech, kde je bit buď - anebo, může *n* bitů kódovat jakoukoli z 2^n hodnot. Qubity mohou kódovat tyto booleovské hodnoty spolu se všemi jejich možnými superpozicemi. To dává kvantovému počítači potenciál k paralelnímu zpracování, jež nemá klasickou obdobu. Kvantové počítače tedy teoreticky mohou řešit určité skupiny problémů, o kterých by se jinak soudilo, že jsou výpočetně neřešitelné.

Příkladem je hledání prvočíselného rozkladu obrovských čísel. Je to klíč k prolomení dnes nejrozšířenějších kryptografických algoritmů, konkrétně šifry s veřejným klíčem RSA,[31] na které závisí světový internetový obchod. Funguje tak, že obrovské číslo (součin dvou prvočísel) je vlastně veřejným klíčem k zašifrování zprávy - pokud by odposlouchávající přišel na jeho prvočísla (rovněž obrovská), dokáže zprávu rozluštit. Vtip je v tom, že vynásobení páru obrovských prvočísel je snadné, ale opačná cesta (faktorizace čili rozklad na původní činitele) je mimořádně obtížná. Postup je informační jednosměrkou. Faktorizace RSA čísel je tedy pro klasické počítače velkou výzvou. V prosinci 2009 použila skupina vědců z Lausanne, Amsterodamu, Tokia, Paříže, Bonnu a Redmondu v USA mnoho set strojů, které po téměř dvou letech práce zjistily, že číslo

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

je součinem čísel

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948927

a

6746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917.

Odhadli, že při výpočtu provedli více než 10^{20} aritmetických operací.[32]

Toto číslo bylo přitom jedno z menších RSA čísel; kdyby předložili řešení o něco dříve, mohli vyhrát 50 000 dolarů, které jako hlavní cenu nabídly RSA Laboratoře. Pokud jde o klasické výpočetní procesy, takové šifrování se považuje za poměrně bezpečné. Větší čísla zaberou exponenciálně více času, který v určitém okamžiku přesáhne věk vesmíru.

Kvantové počítání je něco jiného. Schopnost kvantového počítače zaujímat současně mnoho stavů otevírá nové obzory. V roce 1994, kdy ještě nikdo nevěděl, jak vlastně sestavit jakýkoli kvantový počítač, zjistil jeden matematik z Bell Labs, jak takový kvantový počítač naprogramovat, aby se vyřešil problém

prvočíselného rozkladu. Byl to Peter Shor, génius na řešení problémů, jenž rychle vyhrával matematické olympiády a různé soutěže. Svůj důmyslný algoritmus, který posunul hranice tohoto oboru, nazval jednoduše „faktorizační algoritmus" - všichni ostatní ho znají jako „Shorův algoritmus". Za dva roky, rovněž v Bell Labs, přišel Lov Grover s kvantovým algoritmem k prohledávání obrovské netříděné databáze. To pro svět neomezené informace znamená kanonický těžký problém - hledání jehly v kupce sena.

Dorit Aharonovová z Hebrejské univerzity sdělila v roce 2009 posluchačům: „Kvantové počítače znamenaly v podstatě revoluci. Vyvolal ji Shorův algoritmus. Ale *důvod* revoluce - kromě úžasných praktických důsledků - je ten, že znovu definují, co je *snadný* a co *těžký* problém."[33]

To, co dodává kvantovým počítačům jejich schopnosti, zároveň způsobuje, že je s nimi nesmírně obtížné pracovat. Získat informaci ze systému znamená pozorovat ho, a pozorovat systém znamená zasahovat do kvantových kouzel. Qubity nelze pozorovat, jak paralelně provádějí exponenciálně mnoho operací - při pokusu změřit tuto stínovou síť možností qubit zkolabuje na běžný bit. Kvantová informace je křehká. Zjistit výsledek výpočtu lze jedině tak, že člověk počká, až kvantová práce skončí.

Kvantová informace je jako sen - vždy mizí, nikdy neexistuje tak stále jako slovo vytištěné na stránce. Bennett uvádí: „Mnoho lidí může po přečtení knihy pochopit stejné poselství, ale snažit se říci druhým o vašem snu mění vaše vzpomínky na něj, až nakonec svůj sen zapomenete a pamatujete si jen to, co jste o něm řekli."[34] Kvantový kolaps se zase rovná opravdovému anulování činnosti: „Lze po právu říci, že i Bůh zapomíná."

Shannon sám se již nedožil květů ze semínek, která zasadil. Bennett si myslí: „Kdyby zde Shannon teď byl, domnívám se, že by ho nadchla kapacita kanálu, kterou navíc ještě podporuje provázání. Stejná forma, zobecnění Shannonovy věty, velmi elegantně zahrnuje klasické i kvantové kanály. Standardně se tedy uznává, že kvantové zobecnění klasické informace vedlo a vede k průzračnější a působivější teorii výpočetních procesů i komunikace."[35] Shannon zemřel v roce 2001 a poslední roky prožil v kalném šeru, když ho od světa izolovala nemoc, která vymaže všechno - Alzheimerova choroba. Jeho život překlenul 20. století, které pomohl definovat. Víc než kdokoli jiný byl Shannon zakladatelem věku informace. Kyberprostor je částečně jeho výtvorem - nikdy ho nepoznal, třebaže ve svém posledním rozhovoru v roce 1987 řekl reportérovi, že zkoumá ideu zrcadlových místností: „aby přišel na veškeré možné zrcadlové místnosti, které jsou smysluplné v tom, že kdybyste se z jedné podívali kolem, prostor by byl rozdělen na shluk místností a vy byste se nacházeli v kaž-

dé z nich; a takto by to bez rozporu pokračovalo až do nekonečna."[36] Chtěl ve svém domě poblíž MIT postavit galerii zrcadel, ale již to neuskutečnil.

Byl to John Wheeler, kdo za sebou zanechal plán rozvoje kvantové informatiky - malý seznam pracovních úkolů pro další generaci fyziků a informatiků.[37] Vybídl je:

- Převeďte kvantové verze teorie strun a Einsteinovy geometrodynamiky z jazyka kontinua do jazyka bitů.
- Vynalézavě zkoumejte jeden po druhém všechny působivé prostředky, kterých matematika - včetně matematické logiky - dosáhla... a pro každou takovou metodu vypracujte přepis do světa bitů.
- *A nakonec*: Litujete toho? Ne, oslavujte, že neexistuje jasná definice pojmu ‚bit' jako elementární jednotky při nastolování smyslu... Když se naučíme, jak kombinovat bity ve fantasticky velkých číslech s cílem získat to, čemu říkáme existence, budeme lépe chápat, co vlastně slovy bit a existence myslíme."

Tato výzva trvá, a nejen pro vědce - nastolování smyslu.

KAPITOLA ČTRNÁCTÁ

PO ZÁPLAVĚ

Velkolepé album Babylonu

Dejme tomu, že v každé knize je ještě jiná kniha a v každém písmenu na každé straně se neustále objevuje další svazek - a tyto svazky nezabírají na stole žádné místo. Dejme tomu, že poznání by šlo smrštit na samotnou podstatu, která by se nacházela v obrázku, znaku, v místě, které místem není.[1]

HILARY MANTELOVÁ (2009)

„Vesmír (kterému jiní říkají knihovna)..."[2]

Těmito slovy začal v roce 1941 Jorge Luis Borges svou povídku s názvem „Babylonská knihovna". Pojednávala o bájné knihovně, ve které jsou všechny knihy ve všech jazycích: knihy apologetické a prorocké, evangelia, komentáře k evangeliím a komentáře k jejich komentářům, knihy s přesným a podrobným průběhem budoucnosti, vsuvky ze všech knih ve všech ostatních knihách, pravý katalog knihovny a nesčetné množství nepravých katalogů. Tato knihovna (které jiní říkají vesmír) skrývá veškeré informace. Přesto tam nelze najít poznání - právě proto, že veškeré poznání tam *je*, uložené mezi veškerým klamem. V zrcadlových galeriích lze na nesčetných policích najít všechno a nic. Neexistuje dokonalejší příklad informačního zahlcení.

My si vytváříme vlastní skladiště. Trvalost informace, to, že je těžké zapomenout, je pro dnešní dobu charakteristické a navyšuje to zmatek. Když on-line encyklopedie zvaná Wikipedie - která je bezplatná, amatérská a založená na spolupráci - předstihla rozsahem všechny světové tištěné encyklopedie, redaktoři si uvědomili, že často jeden název odkazuje na více článků. Vypracovali tedy zásady pro odstraňování nejednoznačností, což vedlo ke vzniku více než 100 000 stránek s rozcestníky. Například uživatel, který se v bludišti anglické Wikipedie pídil po heslu „Babel", se dostal na rozcestníkovou stránku „Babel (disambiguation)". Ta ho pak nasměrovala ke článkům o všem, co lze slovem Babel označit: k hebrejskému názvu dávného Babylonu, k Babylonské věži, ke stejnojmenným irácký novinám, ke knize Patti Smithové, k sovětskému spisovateli, k australskému časopisu pro učitele jazyků, k filmu, k hudebnímu vydavatelství, k australskému ostrovu, ke dvěma horám v Kanadě a k „neutrální planetě ve smyšleném vesmíru Star Treku" a k mnoha dalším. Rozcestníky