DIPLOMOVÁ PRÁCE

Prognóza vývoje kvantových počítačů

Forecast of quantum computers development

STUDIJNÍ PROGRAM

Projektové řízení inovací

VEDOUCÍ PRÁCE

doc. RNDr. Bohumír Štědroň, CSc.

KUCHAŘ

JAN **2022**

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Kuchař** Jméno: **Jan** Osobní číslo: **461048**

Fakulta/ústav: **Masarykův ústav vyšších studií**

Zadávající katedra/ústav: **Institut ekonomických studií**

Studijní program: **Projektové řízení inovací**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Prognóza vývoje kvantových počítačů

Název diplomové práce anglicky:

Forecast of Quantum Computers Development

Pokyny pro vypracování:

Cílem diplomové práce je přiblížit pojem kvantových počítačů, provedení prognózy vývoje kvantových počítačů. Přínosem práce je prognóza vývoje kvantových počítačů a důsledky implementace této technologie. Osnova: 1. Úvod 2. Teoretická část: Kvantový počítač, historie, vývoj, oblasti využití. 3. Praktická část: Prognostické metody, analýza, prognóza vývoje. 4. Dopady na svět. 5. Závěr.

Seznam doporučené literatury:

1. ŠTĚDROŇ, Bohumír. Prognostické metody a jejich aplikace. C. H. Beck. 2012
2. ŠTĚDROŇ, Bohumír a kol. Právo a umělá inteligence. Aleš Čeněk s. r. o. 2020
3. ŠTĚDROŇ, B., KOCOUR. V. Technologické prognózy a telekomunikace. Sdělovací technika. 2014
4. LE BELAC M. Short Introduction and Quantum Computation. Cambridge University Press, 2006

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. RNDr. Bohumír Štědroň, CSc., FD ČVUT

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **25.01.2021** Termín odevzdání diplomové práce: **20.08.2021**

Platnost zadání diplomové práce: **19.09.2022**

doc. RNDr. Bohumír Štědroň, CSc.	Mgr. František Hřebík, Ph.D.	prof. PhDr. Vladimíra Dvořáková, CSc.
podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání

Podpis studenta

Kuchař, Jan. Prognóza vývoje kvantových počítačů. Praha: ČVUT 2022. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citoval a uvádím je v přiloženém seznamu použité literatury. Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: 06. 01. 2022 Podpis:

Poděkování

Rád bych poděkoval doc. RNDr. Bohumírovi Štědroňovi, CSc. za cenné rady, pomoc, ochotu, podporu a odborné vedení, které mi bylo poskytováno při zpracovávání mé diplomové práce. Dále děkuji své rodině a všem blízkým za jejich psychickou podporu, trpělivost a rady během vypracovávání práce.

Abstrakt

Cílem práce je přiblížení pojmu kvantových počítačů a provedení prognózy vývoje kvantových počítačů za účelem zjištění, kdy pocítíme dopady v běžném životě. Na začátku práce vysvětluji fungování kvantových počítačů. Poté následuje stručná historie kvantových počítačů, za kterou je popsán hardware kvantových počítačů. Následují možnosti jejich praktického využití. Představím společnosti, které je vyvíjí. Za pomocí krátkého dotazníku ukážu povědomí studentů o kvantových počítačích. Popíšu prognostické metody a provedu analýzu prostředí. Po prognóze vývoje kvantových počítačů následují dopady na svět a závěr práce.

Klíčová slova

Technologické prognózy, prognostika, prognostické metody, kvantové počítače, vývoj

Abstract

The aim of the work is to approach the concept of quantum computers and forecast the development of quantum computers in order to find out when we will feel the impact in everyday life. At the beginning of the work, I explain how quantum computers work. This is followed by a brief history of quantum computers, after which is the description of the quantum computers hardware. The possibilities of their practical use follow. I will introduce corporations that develop them. Using a short questionnaire, I will show students awareness of quantum computers. I will describe forecast methods and analyze the environment. The forecast of the development of quantum computers is followed by impacts on the world and the conclusion of the work.

Key words

Technological forecasts, forecasting, forecasting methods, quantum computers, development

OBSAH

TEORETICKÁ ČÁST

1 ÚVOD

Richard Feynman byl přesvědčen o tom, že nikdo nerozumí kvantové mechanice. Ani on sám. Jako průkopník kvantových počítačů byl o tomto přesvědčen. Sám tedy nemohu prohlásit, že bych kvantové mechanice rozuměl, ale pokusil jsem se alespoň porozumět hardwaru, který na těchto principech pracuje.

O kvantových počítačích slyšíme čím dál častěji ve spojení s objevy nebo novými rekordy. Jak to s nimi doopravdy je? A je vlastně o co stát?

V této práci se pokusím čtenáři přiblížit pojem kvantový počítač v neinvazivní formě. Vysvětlím, na jakém principu kvantové počítače pracují. Čím si musela projít teorie, než se kvantové počítače začaly stavět. Přiblížím vám experimentální architekturu kvantových počítačů a možná využití těchto počítačů v budoucnosti. Následovat bude představení největších společností, které pracují na vývoji hardwaru kvantových počítačů. Poté popíšu prognostické metody. Udělám analýzu zemí, které se na vývoj kvantových počítačů zaměřují. Provedu analýzu společností s cílem zjištění největšího průkopníka v této technologii. Ten by měl poukázat na to, jakým směrem se budou kvantové počítače pohybovat do budoucna za pomocí prognostické metody časových řad a zhodnotím dopady na svět v budoucnosti.

2 KVANTOVÝ POČÍTAČ

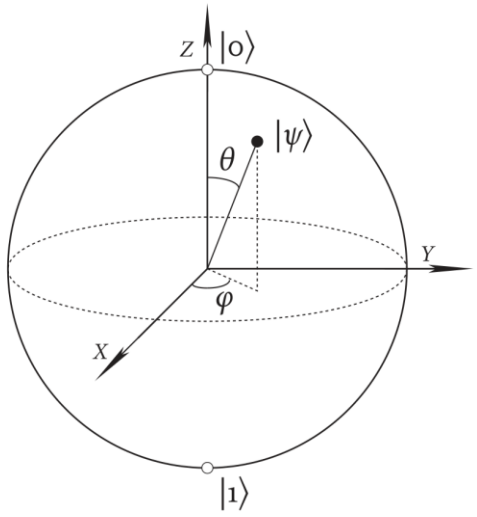
V dnešní době máme po ruce výkonné počítače ve formách mobilního telefonu, stolního počítače, laptopů a tabletů. Když se podíváme na jejich historický vývoj z pohledu výkonu, tak můžeme poměrně s klidem říct, že Gordon E. Moore měl pravdu. Jeho předpověď, že se každým rokem zdvojnásobí počet tranzistorů na jednom integrovaném obvodu, zněla v tu dobu těžko dlouhodobě udržitelná. Moorův zákon, i přesto, že o zákon nejde, nám dlouho poukazoval na přibližný vývoj elektroniky k nárůstu výkonu a úsporách potřebné energie. V této době už se blížíme k samotným fyzikálním limitům velikosti tranzistorů (2). Abychom porozuměli rozdílům mezi klasickým tranzistorovým počítačem a jeho kvantovým protějškem, tak je nejdříve nutné vědět, jak pracuje klasický počítač.

Klasický počítač pracuje na bázi bitů. Bit může mít jednu ze dvou hodnot 1 nebo 0. Z praktického hlediska se dají brát jako ano a ne. S použitím logických členů vytváříme pomocí programovacích jazyků vše, na co jsme dnes zvyklí v počítačích, mobilech a dalších elektronických zařízeních. Tímto typem tranzistorové architektury lze vyrobit v softwaru prakticky vše, co potřebujeme, ale i tak narážíme na určitá omezení. Jak už bylo řečeno, výrobní procesy tranzistorů se blíží k fyzikálním limitům, to znamená, že navyšování výkonu, jen přidáváním dalších tranzistorů nebude možné. Je to díky tomu, že při určité velikosti, asi 10^{-9}m se začnou objevovat kvantově mechanické efekty, při kterých již tranzistory nebudou fungovat spolehlivě. Tedy alespoň u domácích počítačů, protože když se podíváme na superpočítače, tak zjistíme, že u nich je toto řešení běžné. Za pomocí propojení masivního množství procesorů získáváme ty početně nejvýkonnější počítače na světě. U kvantových počítačů jde oproti těm klasickým o navyšování výkonu exponenciálně. Běžný počítač si lze představit jako 2n kde n je počet tranzistorů. Přírůst výkonu tedy bude lineární. Kvantové počítače si představujeme jako 2^n, kde n je počet kvantových bitů. Výkon poté roste exponenciálně.

U kvantových počítačů tyto bity fungují jinak než u počítačů klasických. Říkáme jim proto kvantové bity nebo qubity (quantum bit). Představme si klasický bit jako minci. Každá mince má dvě strany. První stranu budeme brát jako 1 a druhou jako 0. Minci můžeme otáčet a pokaždé, když jí položíme například na stůl, tak bude mít jen jednu hodnotu. Pokud bychom vzali těchto mincí více a vyskládaly je vedle sebe, tak bychom z nich mohli za pomocí otočení vytvořit určitou zprávu. Více bitů správně složených za sebou by vyjadřovalo například písmeno. Přidejme více mincí/bitů a může jít o obrázek, písničku nebo o prakticky cokoliv. Takto bych vysvětlil fungování bitů v klasickém počítači. Nyní si představme stejnou minci. Tuto minci místo toho, abychom jí na stůl položili, tak jí roztočíme. Jakou hodnotu pak tato mince má? 1 nebo 0? Mohli bychom říct, že žádnou nebo obě. Ano, může to znít zvláštně, ale kvantový bit funguje na podobné bázi (3). Qubit má prakticky padesátiprocentní šanci na to být 1 nebo 0. Když se tato mince točí tak je zároveň hodnotou 1 a 0. Tomuto jevu se říká superpozice. Dalším jevem kvantových bitů je kvantová provázanost neboli entanglement. Pokud jsou spolu dva qubity provázány, tak díky fyzikálním vlastnostem tohoto jevu sdílí svou hodnotu. Když má jeden z těchto dvou kvantových bitů

hodnotu 1, tak ho má i ten druhý. V praxi to pro nás může vypadat absurdně. Představme si dvě černé krabičky. V každé z nich je jeden qubit a tyto dva qubity byly provázány. Jednu krabičku můžeme nechat na zemi a druhou vezmeme například na druhou stranu vesmíru. Ano, jde o extrémní příklad, ale fungovat by měl. Netušíme, jestli jsou tyto kvantové bity v hodnotě 1 nebo 0. Pokud bychom jednu krabičku otevřeli a zjistili, že je hodnota 1, tak bychom naměřili stejnou hodnotu u krabičky druhé. Tomuto jevu se říká kvantová teleportace a mohl by být průlomový pro zabezpečenou komunikaci.

U obrázku 1 můžeme vidět reprezentaci qubitu za pomocí Blochovy koule. Kvantový bit $|\psi\rangle$ je vyobrazen z hlediska dvou úhlů θ a ϕ. θ se pohybuje mezi 0 a π. Φ se pohybuje mezi 0 a 2π. Tímto jsem chtěl poukázat na to, že mince patří jen k jednoduchému vysvětlení. Často se qubity zobrazují jako 2D amplitudy.



Obrázek 1: Blochova koule, Zdroj:(4) str. 57

3 HISTORIE KVANTOVÝCH POČÍTAČŮ

1905 – Albert Einstein vysvětlil fotoelektrický efekt (svícení světla na specifické materiály může fungovat k vypuštění jeho elektronů) a navrhl možnost, že se světlo skládá z fotonů nebo kvantových částic

1924 - Termín Kvantová mechanika byla poprvé použita Maxem Bornem v jeho práci

1925 až **1927** – Werner Heisenberg a Niels Bohr vytvořili dodnes běžně vyučovanou Kodaňskou interpretaci kvantové mechaniky

1930 – Paul Dirac vydal učebnici Principy kvantové mechaniky, která se stále využívá

1935 – Albert Einstein, Boris Podolsky a Nathan Rosen vydali článek, ve kterém zdůrazňují neintuitivní povahu kvantových superpozic, a že popis fyzické reality poskytovaný kvantovou mechanikou není úplný (EPR paradox)

1935 - Vznikl myšlenkový experiment známý jako Schrödingerova kočka při rozhovorech mezi Erwinem Schrödingerem a Albertem Einsteinem; objevuje se díky němu také termín kvantové zapletení (quantum entanglement)

1947 - V dopise Maxovi Bornovi poprvé Albert Einstein odkazuje na kvantové zapletení jako “spooky action at a distance ” (strašidelná akce na dálku)

1980 – Paul Benioff vydává dokument, který popisuje kvantově mechanický model Turingova stroje (teoretický model počítače)

1981 – Richard Feynman tvrdí, že oproti klasickému počítači by měl mít kvantový počítač potenciál simulovat fyzikální jevy

1985 – David Deutsch dal dohromady popis kvantového Turingova stroje

1992 – Deutsch–Jozsa se stal jedním z prvních příkladů kvantového algoritmu, který je exponenciálně rychlejší než klasický algoritmus

1993 – Byla vydána práce popisující myšlenku kvantové teleportace

1994 – Peter Shor vytvořil kvantový algoritmus pro faktorizaci celých čísel, který má potenciál dešifrovat komunikaci zabezpečenou pomocí RSA, což je běžná metoda zabezpečení dat

1996 – Lov Grover vymyslel algoritmus vyhledávání v kvantové databázi

1998 – První demonstrace korekce kvantových chyb; první důkazy, že je možné kvantové výpočty emulovat na klasických počítačích

1999 – Yasunobu Nakamura a Jaw-Shen Tsai poukazují na to, že lze využít supravodivý obvod jako kvantový bit

2002 – První verze plánu kvantové výpočetní techniky s klíčovými výzkumníky

2004 – Zapletení prvních pěti fotonů čínskou skupinou pod vedením Jian-Wei Pana

2011 – První komerčně dostupný kvantový počítač od společnosti D-Wave

2012 – Založena první společnost specializovaná na softwarový vývoj pro kvantové počítače 1QBit

2014 – Bezchybná teleportace informací mezi dvěma qubity vzdálenými přibližně 3 metry od sebe

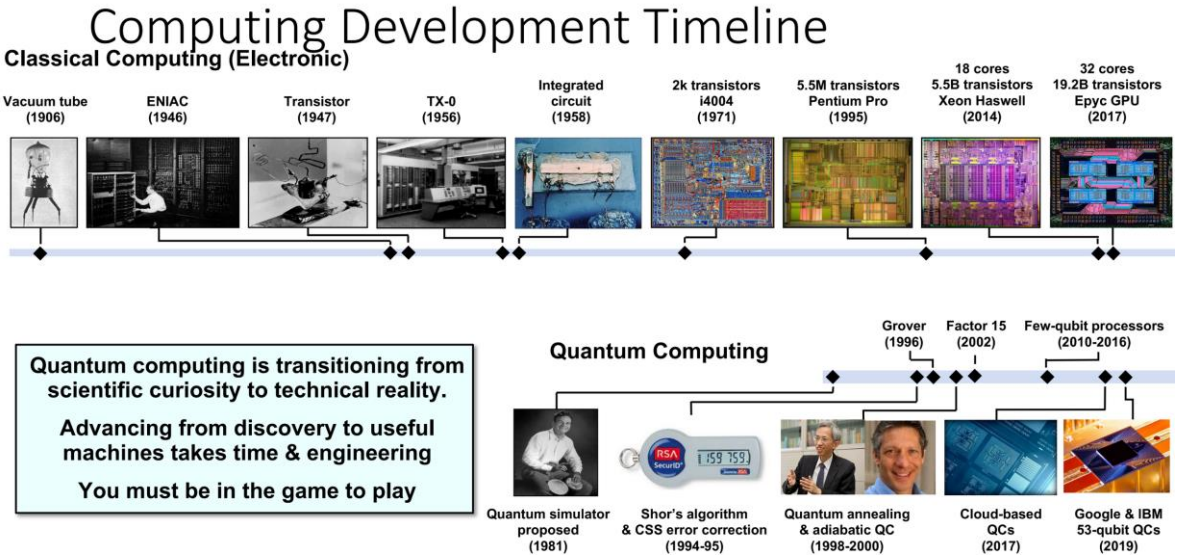
2017 – První kvantová teleportace nezávislých jednofotonových qubitů čínskými vědci na satelit v nízké oběžné dráze do vzdálenosti až 1400 km

2019 – Google tvrdí, že dosáhl kvantové nadvlády (6)

2020 – IonQ tvrdí, že postavilo zatím nejsilnější kvantový procesor technologií iontové pasti s 32 qubity (36);

2021 – IBM představilo 127 qubitový procesor Eagle (65)

Na obrázku 2 můžeme vidět časovou linii počítačového vývoje. Ve vrchní části časové osy je zobrazen postup klasických počítačů od elektronky přes tranzistor k integrovanému obvodu až k současným procesorům s více jádry. Ve spodní části se nám ukazuje vývoj kvantových počítačů. Je tedy rozhodně vidět, že kvantové počítače jsou stále v začátcích vývoje. Naštěstí se některé zkušenosti z klasických počítačů promítají do vývoje těch kvantových, což k dozrávání této technologie velmi napomáhá.



Obrázek 2: Časová osa vývoje počítačů, Q2B prezentace William Oliver, Zdroj: (2)

4 VÝVOJ KVANTOVÝCH POČÍTAČŮ

Kvantové počítače můžeme brát jako poměrně mladé odvětví, kterému je věnována pozornost posledních 20 let. Tato pozornost však nebyla zdaleka tak intenzivní, jako je v posledních letech. O průlomech ve vývoji hardwaru a v posledních letech dokonce softwaru se můžeme dozvídat i z nespecializovaných webů. Každým rokem se kvantové technologie zlepšují a závod o nejvýkonnější, nejspolehlivější a o obecně nejvyužitelnější je neúprosný. V této kapitole se zaměřím na možnosti implementace kvantových bitů. Na některých technologiích se společnosti shodli a snaží se o jejich nejlepší implementaci. Neznamená to však, že se tyto společnosti trefili do černého. Je totiž šance, že vývoj bude zastaven z důvodů, které se nedali předem předpokládat. Jiné společnosti sází přesně na to. Vyvíjí proto jiné možnosti aplikování qubitů.

Největším problémem, s kterým se vývoj kvantových počítačů potýká je dekoherence. Jde o nepřesnosti kvantových bitů z důvodu reakce na okolní prostředí. Zároveň se díky dekoherenci určuje, jak dlouho dokáže být qubit propletený bez ztráty informace. Proti této nesoudržnosti se v současné době vyvíjení techniky korekce chyb. Dosáhnout by se této korekce mělo za pomocí většího množství kvantových bitů. Při velkém množství qubitů by většina z nich pracovala právě na kontrole, opravě chybovosti systému.

V roce 2000 sepsal teoretický fyzik David P. DiVincenzo pět kritérií pro funkční kvantový počítač:

- Škálovatelný systém s dobře charakterizovanými qubity
- Schopnost inicializovat stav qubitu do jednoduchého výchozího stavu
- Relevantně dlouhá doba dekoherence
- Univerzální set kvantových hradel
- Možnosti měření specifických pro qubit (45)

K tomu, abychom mohli mít reálné a praktické kvantové počítače, tak je potřeba vyřešit nespočet problémů. Asi tím nejsložitějším je dekoherence. Při dekoherenci qubit interaguje s něčím v prostředí, co nepatří k výpočtům. Potřebujeme qubit v jeho základním stavu a udržet ho tak do té doby, dokud ho nebudeme využívat. Samozřejmě k tomu, abychom mohli dělat výpočty, musíme zahrnout logické členy a obvody.

Vybrané architektury kvantových bitů patří k těm nejdiskutovanějším a nejpoužívanějším. Tím samozřejmě typy qubitů zdaleka nekončí. Kvantové vlastnosti můžeme pozorovat i v reálném životě, a proto je důležité si uvědomit, že možností aplikace jsou mnohem širší.

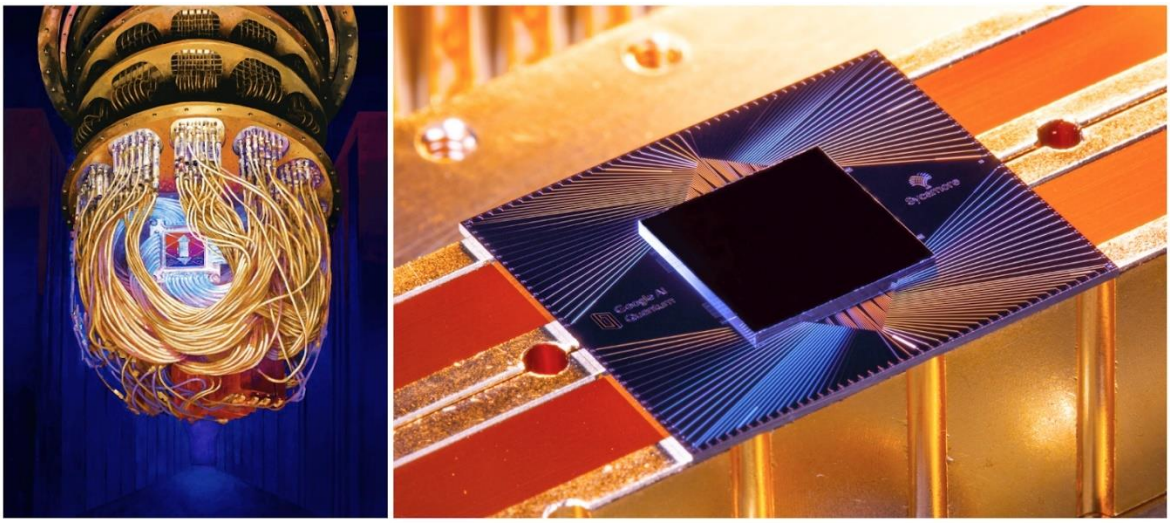
Tyto různé typy kvantových bitů otevírají možnosti a přináší naději pro vytvoření plnohodnotného kvantového počítače. V komerční sféře, ale samozřejmě nejde jen o tyto objevy. Společnosti potřebují využít svých postupů ve vývoji k přesvědčení veřejnosti, že právě oni jdou tou správnou cestou vývoje kvantového počítače. Jak by se ale mohly tyto počítače porovnávat, když každá typologie má jiné vlastnosti? Pro některé se jednalo o číslo qubitů v jejich počítači, později se začalo objevovat heslo kvantového objemu. Kvantový objem je jedno číslo, které zachycuje výkon současných kvantových počítačů. Tento protokol testuje, jak dobře dokáže kvantový počítač provozovat obvod, který se skládá z dvouqubitových bran působících paralelně na podmnožinu qubitů zařízení. Kvantový objem prakticky identifikuje největší obvod čtvercového tvaru, který dokáže běžet na daném počítači. S tímto měřítkem však nejsou všechny společnosti spokojeny a vydávají čísla kvantového objemu prakticky jen pokud jde o překvapivě velké číslo. (46)

V současnosti se největší společnosti zabývají vývojem počítačů na základě NISQ (Noisy Intermediate-Scale Quantum). Teoretický fyzik John Preskill napsal v roce 2018 článek popisující éru, ve které bude vývoj kvantových počítačů na úrovni padesáti až pár set kvantových bitů. Padesát kvantových bitů z důvodu dosažení přibližné úrovně, kde si kvantové simulace již s problémem neporadí v krátkém časovém horizontu. Tomuto jevu se často říká kvantová nadvláda. Slovo hlučný (Noisy) poukazuje na neúplnou kontrolu nad kvantovými bity. Hluk, který narušuje kvalitu výpočtů qubitů může přicházet prakticky ze všeho a bude limitovat to, co kvantové počítače dokážou v blízké budoucnosti. Podle Preskilla je důležité nebrat éru NISQ jako katalyzátor ke změně světa, ale měla by se brát jako krok k výkonnějším technologiím. U kvantových počítačů se nezajímáme jen o počet qubitů, ale také o jejich kvalitu neboli jejich přesnost, se kterou dokáží počítat, a se kterou se jim daří proplétat. V současné době jsou nejrozvinutějšími typy hardwaru pro kvantové počítače supravodivé okruhy a uvězněné ionty. Chybovost dvouqubitového hradla bývá často na úrovni jedné desetiny až jedné setiny procenta. Preskill píše, že neočekává možnost vykonání okruhu s více jak tisíci hradly (prakticky tisíc dvou qubitových operací). Důvodem je to, že hluk u takto velkých obvodů přemůže signál. (47) Společnosti však tato varování ignorují a snaží se přijít s masivními korekcemi chyb, které by dostalo tyto okruhy k dostatečné pravdivosti výstupu. Za pomocí více qubitů se pokusí sestavit jeden qubit, takzvaný logický. Tento qubit bude mít díky kvantové korekci chyb minimální chybovost. Je však náročné říct, kolik těchto kvantových bitů bude potřeba k jednomu logickému.

Typů hardwaru pro tvorbu kvantových počítačů je velké množství a v současnosti se objevují nové teorie využití. O jakých typech kvantových bitů můžeme slyšet od největších společností, které pracují na vývoji této moderní technologie?

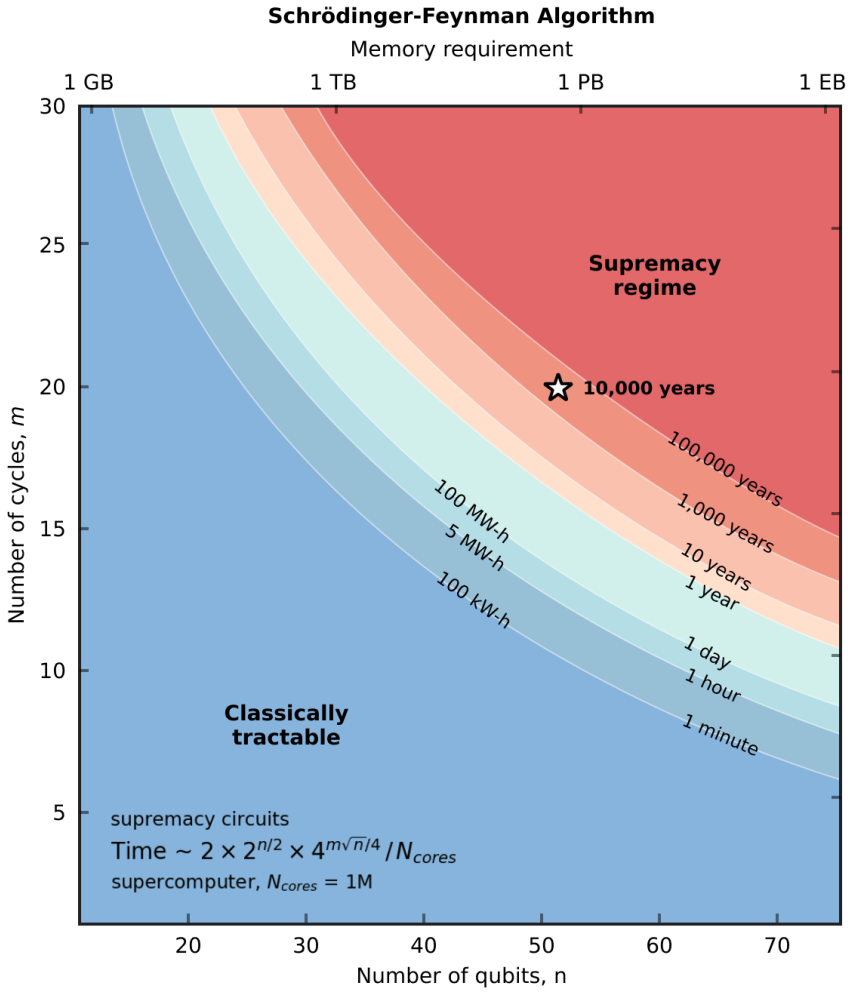
4.1 Supravodivé kvantové bity

Jde o nejvíce rozšířený a používaný typ architektury kvantového procesoru. Fungují na podobné bázi jako dnes známé běžné počítače. Aby se tyto bity chovali jako kvantové, je nutné procesory zchladit k téměř absolutní nule. IBM představilo v roce 2016 pěti-qubitový procesor, který zpřístupnili všem zdarma skrze cloud. Kdokoliv může navrhnout svůj obvod, pokud využívá pět nebo méně kvantových bitů, a spustit ho na jejich počítači. Na konci roku 2017 IBM zpřístupnilo 20 qubitový počítač, ten však již nebyl zdarma. Byl vytvořen pro komerční využití, kde si společnosti mohli zaplatit přístup. V roce 2019 Google oznámil, že dosáhl kvantové nadřazenosti za pomocí svého 53 qubitového Sycamore procesoru. Google tvrdí, že jejich procesor dokončil úkol za 200 sekund. Stejný úkol by prý trval superpočítači 10000 let. (1)



Obrázek 3: Google Sycamore procesor, Google, zdroj: (1)

Na konci roku 2021 společnost IBM překročila hranici 100 kvantových bitů za pomocí procesoru Eagle, který obsahuje 127 qubitů (65)



Obrázek 4: Kvantová nadřazenost, Google, zdroj: (5)

Odhad klasického výpočetního času při 1M CPU jader pro obvody kvantové nadvlády. n-počet qubitů; m-počet cyklů pro Schrödinger-Feynmanův algoritmus. Hvězda ukazuje přibližný čas výpočtu. (5)

4.2 Iontová past

První kvantové logické hradlo bylo demonstrováno v roce 1995 za pomocí iontové pasti. Od té doby se tato technologie nesmírně posunula ke škálovatelnosti a nižší chybovosti.

Další metoda využívá energii iontů. Ion-trap, neboli iontová past, využívá elektromagnetická pole k udržení iontů na své pozici. K udržení této pasti musí být minimalizovány jakékoliv vibrace. Toho dosahujeme chlazením za pomocí laserů k téměř absolutní nule. Úrovně energie iontů zakódují qubity a za pomocí laserů s nimi lze manipulovat. V roce 1995 využil David Wineland iontových pastí k vytvoření prvního CNOT hradla (podmíněná negace), za což mu byla udělena Nobelova cena. V roce 2016 výzkumníci NIST provázali (entangled) více jak 200 iontů beryllia. Ion-traps mají velký potenciál. Na jejich vývoji pracují v současnosti velké společnosti jako Honeywell nebo IonQ. (1)

4.3 Fotonové

Fotony mají výhodu v tom, že je poměrně jednoduché je mezi sebou zaplést (entanglement). Další jejich výhodou je to, že moc neinteragují s okolím, takže vydrží dlouho koherentní. Tyto vlastnosti dělají fotony ideální pro komunikaci, ale bohužel přináší i problematiku při stavění kvantových obvodů. (1) Tento typ hardwaru využívá společnost Xanadu.

4.4 Elektronový spin

Spin elektronu uvězněný v syntetickém diamantu, s kterým se manipuluje za pomocí laserů. U tohoto typu je hlavním problémem škálovatelnost. Podobně se zkoušel spin s jádrem, ale naskytl se stejný problém. (1)

4.5 Kvantové annealery

Kanadská společnost D-Wave již léta prodává kvantové počítače. Jejich nejnovější počítač Advantage má 2.5 krát více meziqubitových spojení a více jak dvojnásobek kvantových bitů oproti jejich předchozímu systému D-Wave 2000Q. Má více než 5000 qubitů, doopravdy je to tak, avšak ne všechny kvantové bity jsou si rovny. Kvantové annealery řeší specifické problémy. Využívají se při optimalizacích a při vzorkování. Při optimalizacích se pracuje s velkým množstvím dat a snaží se zjistit optimální řešení daného problému za pomocí minimálního odporu. Dosahuje těchto výsledků efektivněji díky kvantovému tunelování. Oproti předchozím typům hardwaru zde není cílem dokonale ovládat kvantové bity. Díky tomu je možnost škálování mnohem jednodušší. Společnost D-Wave prodává své počítače velkému množství společností. (1) Mezi nimi je například Volkswagen, který za pomocí tohoto počítače optimalizoval provoz v Lisabonu. (7)

4.6 Topologické kvantové bity

V systému topologických kvantových bitů mají operace na fyzických qubitech extrémně vysokou věrnost díky topologické symetrii implementované na mikroskopické úrovni, kde se korekce chyb řeší za pomocí qubitu samotného. Pomocí této techniky by se teoreticky mohla eliminovat korekce kvantových chyb. Teorie této technologie zní úžasně, ale tato platforma patří mezi nejméně vyvinutou. Stále jde o technologii, která je ve fázi základních experimentů při tvorbě struktur kvantových bitů. Pokud se tyto experimenty povedou a bude možné qubity kontrolovat v laboratorním prostředí, tak za pomocí odolnosti k chybám těchto qubitů může dojít ke škálování této technologie rychleji než u jiných přístupů. (8) Vývojem této technologie se zabývá Microsoft.

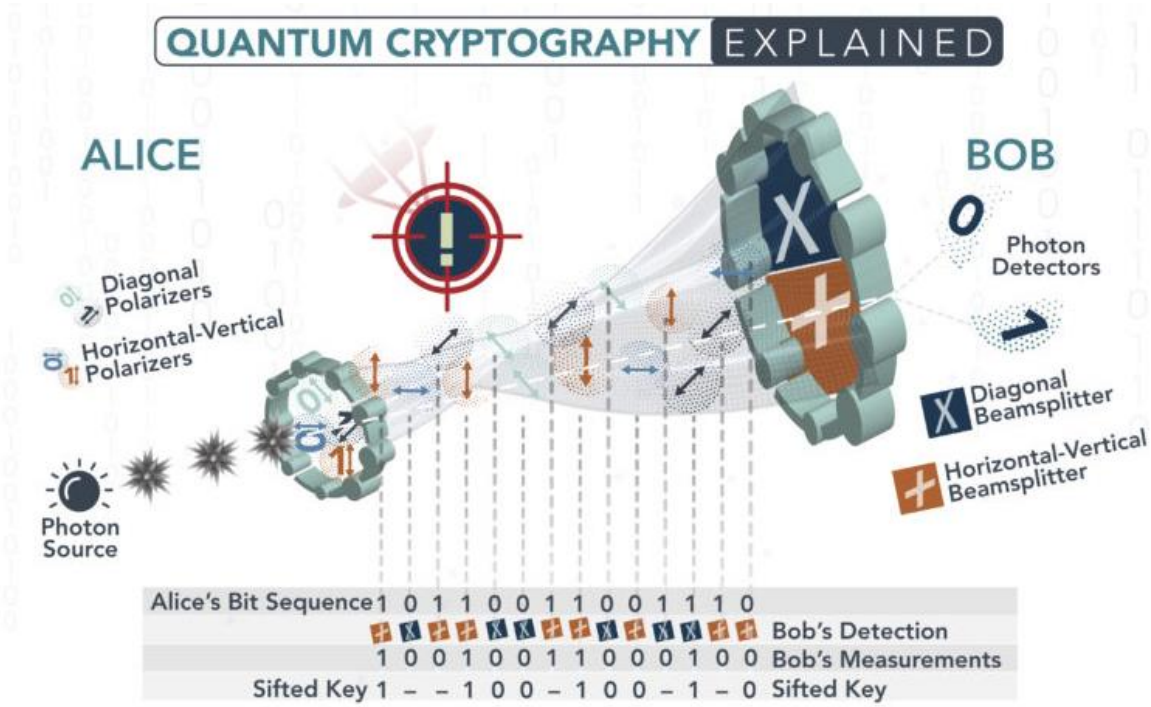
5 VYUŽITÍ KVANTOVÝCH POČÍTAČŮ

Teoreticky by se kvantové počítače mohly využít v široké škále oborů a věřím, že v realitě k tomu také časem dojde. V současnosti jsme však na prahu této technologie, a i přes to, že vývoj se posouvá velmi rychlým tempem dopředu, tak k dosažení funkčnosti extrémně výkonných kvantových počítačů jsme zatím daleko. Nyní se nacházíme stále v době klasických počítačů a rád bych uvedl, že alespoň v blízké budoucnosti nás nečeká jejich nahrazení. Kvantové počítače už z principu fungují na jiné bázi a určité výpočetní procesy by na nich trvali déle než na počítačích klasických. V blízké budoucnosti se však začnou kvantové počítače využívat na specifické úkoly, které zvládnou klasické počítače buďto velmi těžko nebo je nezvládnou vůbec. Mezi takové úkony patří například simulace chemických prvků, která může mít využití ve velkém množství odvětví. V medicíně, ve vytváření nových technologií pro akumulátory, ve vývoji čistších hnojiv nebo jen pro objevování nových sloučenin pro různé účely. V budoucnu nám mohou kvantové počítače zaručit perfektně zabezpečenou komunikaci, silnější zabezpečení dat, kvantový internet a skokové pokroky u strojového učení a umělé inteligence. Dle mého názoru dojde k lepší optimalizaci finančního sektoru a k lepšímu pochopení meteorologie a klimatických změn na Zemi.

5.1 Kvantová kryptografie

S kvantovými počítači přichází výpočetní síla, která by neměla mít problém s prolomením současných metod šifrování. Současná kryptografie veřejných klíčů je z velké části založena na RSA (Rivest-Shamir-Adleman) šifrování. Toto šifrování se využívá při digitálních transakcích jako je například e-mail, ale i u dalších internetových komunikací. Toho se dosahuje za pomoci distribuce symetrických klíčů mezi vzdálenými stranami. Symetrické šifrování se používá z důvodu rychlejšího procesu než při šifrování asymetrickém. Často preferovaný přístup využívá hybridní šifrování, kde se využívá rychlosti sdíleného klíče a zabezpečení systému veřejného klíče pro počáteční výměnu symetrického klíče. Veřejné klíče kryptografických systémů RSA nebo Diffie-Hellman nejsou založeny na určitém matematickém důkazu. Tyto systémy jsou považovány za přiměřeně bezpečné na základě veřejného zkoumání procesu rozdělování velkých čísel na jejich prvočísla. O tomto procesu se říkalo, že je neřešitelný. Dalo by se říct, že v tu dobu, kdy by byl algoritmus prolomen, tak by získané informace neměly již žádnou hodnotu. Síla těchto algoritmů je tedy přímo spojená s tím, že neexistuje známá matematická operace pro rychlou faktorizaci velkých čísel za pomocí výkonu dnešních počítačů. Díky vývoji kvantových počítačů, které by za pomocí Shorova algoritmu propočítaly tuto faktorizaci, přichází problém. V minulosti se prakticky jen navyšovala velikost klíče pro náročnost jeho rozšifrování. Šifrovací algoritmy si tedy snaží držet vždy náskok před sílou počítačového výkonu, aby jeho rozšifrování nebylo jednoduché v krátkém čase. (48)

Kvantová kryptografie přímo závisí na faktorizaci velkých čísel a je založena na základních a neměnných principech kvantové mechaniky. Jedním z nich je Heisenbergův princip nejistoty. Podle něj nelze měřit kvantový stav systému, aniž bychom ho narušili. Druhým principem je fotonová polarizace, tu lze zjistit jen když je tato polarizace měřena. Za pomocí tohoto principu lze kazit pokusy o odposlouchávání. Fotonový filtr se správnou polarizací může detekovat pouze polarizovaný foton, jinak se foton zničí. Při takovýchto principech je tedy možné mít prakticky plně chráněnou komunikaci za pomocí QKD (Quantum key distribution). QKD nabízí techniku k dohodnutí se na sdílené náhodné sekvenci bitů mezi dvěma zařízeními s nízkou šancí na odposlouchávání jinými zařízeními. Takovéto sekvence se poté využívají jako tajné klíče kódování a dekódování mezi danými zařízeními. (48)



Obrázek 5: Grafické znázornění přenosu QKD, zdroj: (49)

Na obrázku 5 máme znázorněnou komunikaci mezi Alicí a Bobem, kteří si chtějí bez narušení poslat tajnou zprávu. Za pomocí QKD pošle Alice Bobovi polarizované fotony přes optický kabel. Kabel nemusí být zabezpečený, protože fotony jsou v náhodných polarizovaných stavech. Pokud se je někdo pokusí odposlouchávat, tak si musí přečíst každý foton, aby tajnou zprávu rozluštil. Poté musí fotony poslat dále Bobovi. Tím, že si odposlouchávač přečetl foton, tak se změní kvantový stav daného fotonu a tím pádem Bob dostane znehodnocený kvantový klíč. Díky tomu jsou Alice a Bob upozorněni, že s klíčem bylo manipulováno a klíče se zbaví. Alice musí zaslat jiný klíč, aby si Bob mohl přečíst tajnou zprávu. (49) V současné době se také pracuje na vývoji takzvané post-quantum kryptografii. Cílem je vyvinout kryptografii, která je odolná vůči rozšifrování jak klasickými počítači, tak také počítači kvantovými. Jde tedy o moderní přístup k šifrování, který nás má připravit na příchod kvantové éry.

5.2 Zdravotní péče

Další využití kvantových počítačů můžeme najít ve zdravotnictví. Jedním z těchto využití je pomoc při diagnostice skenů jako je výpočetní tomografie, magnetická rezonance nebo rentgen. U těchto skenů jsou často výsledky ve špatném rozlišení, mají v sobě hodně šumu. Moderní diagnostické postupy mohou zahrnovat jednobuněčné metody. Například informace o průtokové cytonometrie (měření buněk v pohybu) a sekvenování z jednotlivých buněk vyžadují pokročilé analytické metody, obzvlášť když se jedná o kombinaci dat různých technik. Výzvou je klasifikace buněk podle jejich fyzických a biochemických charakteristik. Tyto charakteristiky jsou důležité při rozlišování buněk normálních od rakovinotvorných. Právě díky strojovému učení u kvantových počítačů by mohla být klasifikace a diagnostika v jednobuněčných metodách mnohem jednodušší a přesnější. Kvantové počítače by mohly pomoci v precizní medicíně. Jde o přizpůsobení léčby na míru jednotlivci. Každý člověk je unikátní a tím pádem reaguje různě na odlišné typy léčby. Individualizovaná medicína vyžaduje započítání aspektů, které jdou nad rámec standardní lékařské péče. Podle průzkumů má lékařská péče podíl jen asi v 10 až 20 procentech na výsledcích léčby. Zbylých 80 až devadesát procent jsou faktory enviromentální a socioekonomické. Toto propojení vytváří výzvy na optimalizaci léčby. Kvantové počítače se také dají využít k výpočtu zdravotního pojištění podle rizik jednotlivců. (50)

Vývoj léků patří mezi velmi diskutovaný potenciál kvantových počítačů. Již v současnosti se používají superpočítače při vývoji nových léků. Kvantové počítače by byly schopny, za pomocí velkého množství dat, hledat jiné, nové sloučeniny, které by bylo možné využít na lepší typy léků. Využití se také najde při klinickém testování bez potřeby testovacích subjektů. Vše bude probíhat na bázi simulace. Časem bychom se mohli dostat k sekvenování a analýze DNA v plné rychlosti. Díky tomu by bylo možné představit pacientům genetická rizika a pomoci lékařům při diagnostice nemocí. (51) Důležitou možností je využití kvantových počítačů při hledání léků na choroby, které stále nejsou léčitelné a zkoumání proteinů při vývoji nových vakcín. To vše jsou oblasti, ve kterých by mohly kvantové počítače přinést pokrok a napomoci nám lidem ke zdravějšímu a delšímu životu.

5.3 Simulace materiálů

Velkým lákadlem pro množství společností v rámci investic do kvantových počítačů je simulace materiálů. Slibují si od toho velké pokroky při hledání optimálních chemických prvků pro své produkty. Jedním z těchto produktů, u kterých je nutná značná inovace do budoucna jsou akumulátory. V současné době máme obří množství technologických produktů, které pracují na nabíjecích cyklech. Mobilní telefony, notebooky, chytré hodinky, bezdrátová sluchátka a čím dál více využívaná elektrická auta. U všech těchto produktů je potřeba inovace akumulátorů. Zvyšující se výkon, kvalita a velikost obrazovek zvyšuje energetické nároky chytrých telefonů. Zvětšování baterií však není řešení. Efektivita, životnost, rychlost nabíjení, výdrž ve stavu nepoužívání jsou možnosti, u kterých se mohou projevit nová chemická složení vyvinutá za pomocí simulací kvantového počítače. Mezi další materiál, který potřebuje vylepšení a dalo by se téměř říct revizi jsou hnojiva. Současná hnojiva mají poměrně značné množství škodlivin a vývoj nových chemikálií, které by při tvorbě nevypouštěly škodliviny by měly dobrý vliv na posun k čistšímu životnímu prostředí. Vylepšení by byla vhodná také u fotovoltaiky. Nalezení vhodnějšího materiálu pro efektivnější tvorbu solární energie. V podobném duchu by mohl pokračovat i vývoj materiálů pro absorpci oxidu uhličitého z atmosféry.

5.4 Strojové učení a umělá inteligence

Je předpokládáno, že jeden z největších dopadů kvantových počítačů bude právě na vývoj strojového učení (machine learning) a umělé inteligence (artificial inteligence). Umělá inteligence je vědním oborem, který se zabývá vytvářením strojů, které vykazují inteligenci. (52) Díky masivnímu výkonu bude kvantový počítač schopen zpracovávat velké množství dat. Tato data se dají využít k přímému učení kvantového počítače. V současné době Google nabízí open-source knihovnu pro kvantové strojové učení. Slouží k rapidnímu prototypování hybridních kvantově-klasických modelů strojového učení. (53) Strojové učení závisí na velkém objemu a vysoké kvalitě dat. Kvantové strojové učení dosahuje mnohem lepšího výkonu při modelování kvantově mechanických systémů než klasické počítače. Díky tomu, že kvantový svět umožňuje superpozici exponenciálně mnoha stavů mohou se qubity pracovat paralelně, tak se dá očekávat, že kvantové počítače budou lépe stavěné na řešení problémů s kvantovými původy. (54) Dá se tedy předpokládat, že pokud budeme zadávat data pro strojové učení kvantovému počítači, tak by mělo jít převážně o data založená na kvantových vlastnostech. Právě kvantové strojové učení vede k objevení nových léků, k vylepšování akumulátorů. Umělá inteligence jde nad rámec strojového učení. Je poměrně jisté, že se nám za pomocí kvantových počítačů povede vybudovat umělou inteligenci na jiné úrovni. Pokud bude doopravdy schopna rozumět kvantové mechanice, tak by nás mohla dovést k úplně novým objevům a pochopení světa.

5.5 Předpověď počasí

Každým rokem se ve světě objevují extrémní vedra, hurikány a jiné velké výkyvy počasí, které se dají jen těžko předvídat a často s sebou přináší spoušť s masivními škodami. Již hodně úsilí bylo věnováno vývoji výpočetních modelů pro zlepšení předpovědí. Při analyzování počasí pro jeho předvídání je využito velké množství dat. Mezi tato data patří tlak vzduchu, jeho teplota a hustota. Při předpovídání klasickými počítači je nutné, aby byl model předpovědi dostatečně rychlý i přes množství dat, co musí zanalyzovat. Předpověď počasí na místní úrovni často stíhá pravidelnější předpovědi, a proto je větší šance na varování při extrémních podmínkách a tím pádem je i možnost zredukovat jejich dopady. Kvantové počítače mají potenciál k analyzování velkého množství dat za významně kratší dobu, než by to trvalo počítači klasickému. Věřím, že v následujících letech se setkáme s pravidelným využíváním kvantových počítačů k předpovědi počasí. Pokud by se nám dařilo předvídat chování počasí, tak by to mělo rozhodně velký dopad na zemědělství, kde právě neočekávané počasí je největší hrozbou. (55)

5.6 Finanční služby

S příchodem plnohodnotných kvantových počítačů také přijdou změny u finančních služeb. Největší změny zaznamenají finanční sektory zabývající se nejistotou a omezenou optimalizací. Dost možná této situace využijí první lidé s přístupem k dostatečně dobře strojově naučenému kvantovému počítači. Takový člověk by dokázal rychle reagovat na změny cenových hladin na trhu za pomocí předpovědí kvantového počítače s širokým přístupem k datům. Takový jedinec by byl na burzovním trhu prakticky nezastavitelný. Samozřejmě v realitě to bude vypadat jinak. Finanční trhy se budou muset na tento vývoj připravit.

Kvantové počítače budou dobře sloužit při cílení a předvídání. Bude možné zjišťovat podvody podle vzoru dat a tyto podvody i do budoucna předvídat. Cílí na zákazníky za pomocí kvantových počítačů, které hledají vzory, klasifikují a provádí předpovědi. Investiční manažeři, kteří optimalizují investiční portfolia do nich nejsou schopni začlenit události v jejich životě, což by kvantový počítač mohl dokázat. Dokázal by také mnohem efektivněji profilovat rizika. (56)

5.7 Kvantový internet

Kvantový internet by podle všeho měl fungovat na podobných principech jako je kvantová kryptografie z kapitoly 7.1. Kvantová komunikační síť je již v provozu a poukazuje na to, jak bude vypadat naše budoucí síť informací. Čínským odborníkům se podařilo zprovoznit první integrovanou kvantovou komunikační síť na světě. Skládá se z více jak sedmi set pozemních optických kabelů a z dvou linek mezi zemí a satelitem. Tato síť přitom pokrývá uživatele v Číně až na vzdálenost 4600 kilometrů. Dosáhl toho tým odborníků Jianwei Pan, Yuao Chen, Chengzi Peng z University of Science A technology of China v Che-feji. Podařilo se jim propojit více než 150 uživatelů, včetně úřadů, bank a energetických sítí. Jianwei pan je přesvědčený, že jde o důkaz použitelnosti kvantových komunikačních sítí pro praktické aplikace ve velkém měřítku. V současnosti pracují na vylepšování této sítě, zrychlují tvorby tajných klíčů QKD a plánují vyvíjet malé a levné QKD satelity, které by umožnili přenos QKD na vzdálenost desítek tisíc kilometrů. (57) (58)

PRAKTICKÁ ČÁST

6 SPOLEČNOSTI

V této kapitole se zaměřuji na přiblížení společností, o kterých se nejvíce mluví ve spojení s kvantovými počítači a jejich hardwarovým vývojem. Určitě není překvapením, že je nejvíce slyšet o velkých zavedených technologických firmách. Je to díky tomu, že se jako jedny z prvních do tohoto budování nové technologie zapojili. V posledních letech se však začaly objevovat nové firmy s jinými technologiemi. Dalo by se říct, že se jedná o závod o to, komu se podaří postavit první plně funkční kvantový počítač s výpočetním výkonem nad rámcem klasických počítačů. Mezi následujícími společnostmi se prakticky neobjevují ty, které se zaměřují jen na specifický problém a okolo něj optimalizují svůj kvantový počítač.

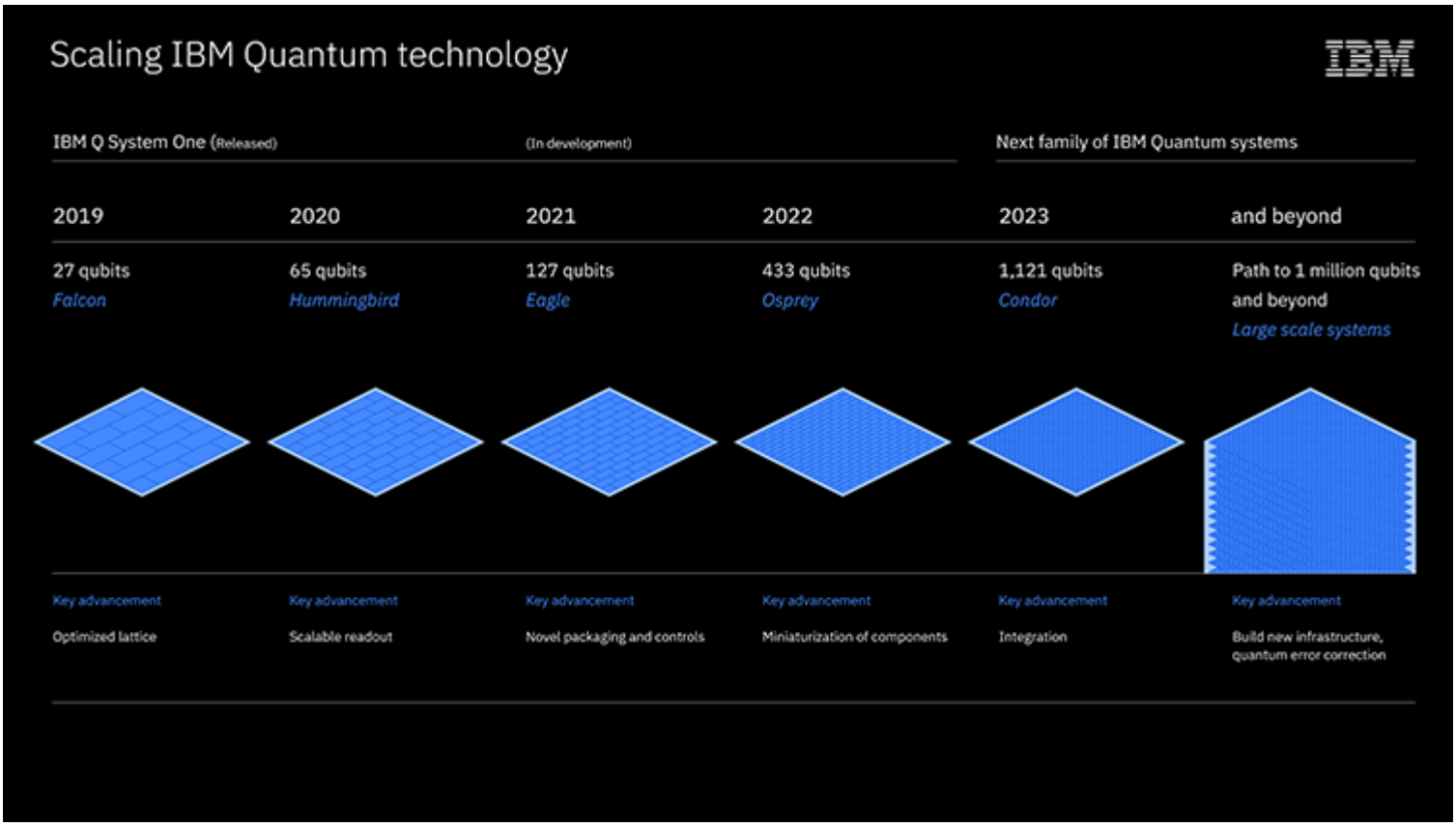
6.1 IBM

Jde o jednu z největších technologických firem s širokou škálou služeb ve světě. Její počátek sahá přibližně 150 let do minulosti, kde byly použity děrovací štítky Americkým úřadem při sčítání lidu. V té době samozřejmě ještě nešlo o IBM (šlo o jiný název). Později IBM pomohlo zajistit sociální pojištění v roce 1935 po jeho uzákonění. Šlo o největší účetnický projekt své doby. V roce 1937 vytvořili stroj na vyhodnocování testů. Později v roce 1952 IBM představilo posun od děrovacích karet k digitálnímu ukládání dat. V roce 1956 Arthur L. Samuel naprogramoval počítač IBM 704 k tomu, aby hrál dámu a učil se. Tato událost je považována za první demonstraci umělé inteligence. V roce 1961 demonstroval William C. Dersch rozpoznání hlasu. Jedná se vlastně o první kroky pro současné umělé inteligence jako je Siri (Apple) nebo Alexa (Amazon). Za pomocí IBM a jejich počítačů a softwaru přistál první člověk na měsíci. Roku 1970 vznikl magnetický pruh, který změnil způsob, jakým jsou přijímány obchodní transakce. Zrodil se nový průmysl, který způsobil revoluci v cestování a přístupu k zabezpečení. První disketa (Floppy disk) vyrobena v roce 1971. UPC (Universal Product Code) byl vymyšlen zaměstnancem Normanem Woodlandem. Jde o kódy, které stále vidíme na prakticky všech baleních produktů. V roce 1980 IBM patentuje přesný laser LASIK, který dokáže psát na lidský vlas. Technologie slouží k operaci očí. IBM vydává svůj první osobní počítač IBM PC v roce 1981. Roku 1997 superpočítač IBM Deep Blue poráží nejlepšího šachistu světa, což je zaznamenáno jako velký krok pro umělou inteligenci. V roce 2011 umělá inteligence IBM Watson dokázala přirozeným porozuměním řeči a kognitivní výpočetní technikou porazit šampiony v televizním kvízu Jeopardy! IBM v roce 2018 představuje superpočítač The Summit se speciálně navrženou architekturou pro umělou inteligenci. Stává se nejvýkonnějším procesorem na světě. A v roce 2019 IBM představuje první komerční kvantový počítač založený na obvodech. (12) Jak můžeme vidět, tak historie IBM je vcelku nabitá vývojovými pokroky. Není potom divu, že by si taková společnost chtěla nechat ujít nový potencionální trh s kvantovými počítači.

Obrázek 6: Logo IBM, zdroj: (12)

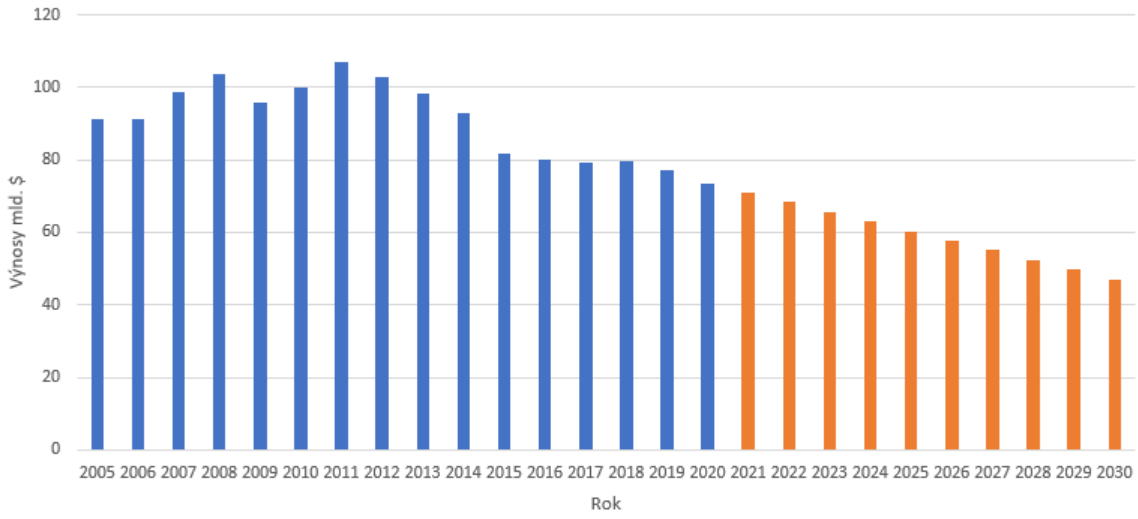
V roce 2019, kdy Google oznámil kvantovou nadřazenost (5) se vůči tomuto oznámení IBM ohradilo. V té době mělo jak IBM, tak Google dostupné kvantové počítače s 53 qubity. Podle Google jejich počítač zvládl vykonat výpočet, který by klasickému počítači trval přibližně 10 tisíc let. Svět byl tímto pokrokem příjemně překvapen a udělal Googlu velkou reklamu. Vědci z IBM však tvrdí, že při ideální simulaci u klasického počítače by tato úloha při vysoké přesnosti byla vyřešena za dva a půl dne. A bylo by možné tento čas ještě zkrátit. Podle IBM tedy Google kvantové nadřazenosti nedosáhl. Kvantová nadřazenost byla popsána Johnem Preskillem v roce 2012 jako moment kdy kvantové počítače dokážou dělat to, co klasické neumí. (14) IBM přišlo se závěrem, že i když jde o masivní pokrok, tak články s nadpisy o dosažení kvantové nadvlády nejsou zcela pravdivé. (13) V současnosti pracuje IBM na vývoji open source programovacího jazyka Qiskit, který pracuje na bázi Python. Snaží se udělat programování kvantových počítačů dostupnějším pro všechny, kteří se o to zajímají.

V roce 2020 představila společnost IBM plán vývoje svých kvantových počítačů. Zde popisují své úsilí o vytvoření kvantových počítačů velkého měřítka. Jejich cílem je do konce roku 2023 zprovoznit 1000 a více qubitový kvantový počítač jménem IBM Quantum Condor. (16) Na konci roku 2021 IBM představilo nový procesor Eagle se 127 kvantovými bity. Jde o druhý procesor, který využívá heavy-hexagonal rozložení pro efektivnější propojení mezi jednotlivými qubity. (65) Dále pracují na nových chladících boxech pro ještě větší počítače. Jejich hlavním cílem je však vytvořit takový kvantový počítač, který bude plně funkční a dostupný pro všechny skrze cloudovou službu. (16)



Obrázek 7: Plán vývoje kvantových počítačů IBM, zdroj: (16)

V obrázku číslo 8 můžeme vidět vývoj výnosů společnosti IBM od roku 2005 do roku 2020. Tento trend poukazuje na snižování výnosů již od roku 2011. V roce 2019 však firma IBM převzala Firmu Red Hat. Tímto poukazuje ještě na silnější zaměření na cloudové služby do budoucna. Pro IBM je důležité, jak se v následujících letech vyvine jejich technologie kvantových počítačů. Mohlo by jít o významnou pomoc při získávání vyšších zisků při jejich komercializaci. Dále je na obrázku provedena předpověď vývoje výnosů společnosti do roku 2030.



Obrázek 8: Předpověď výnosů společnosti IBM, zdroj: (15), vlastní zpracování

6.2 Google

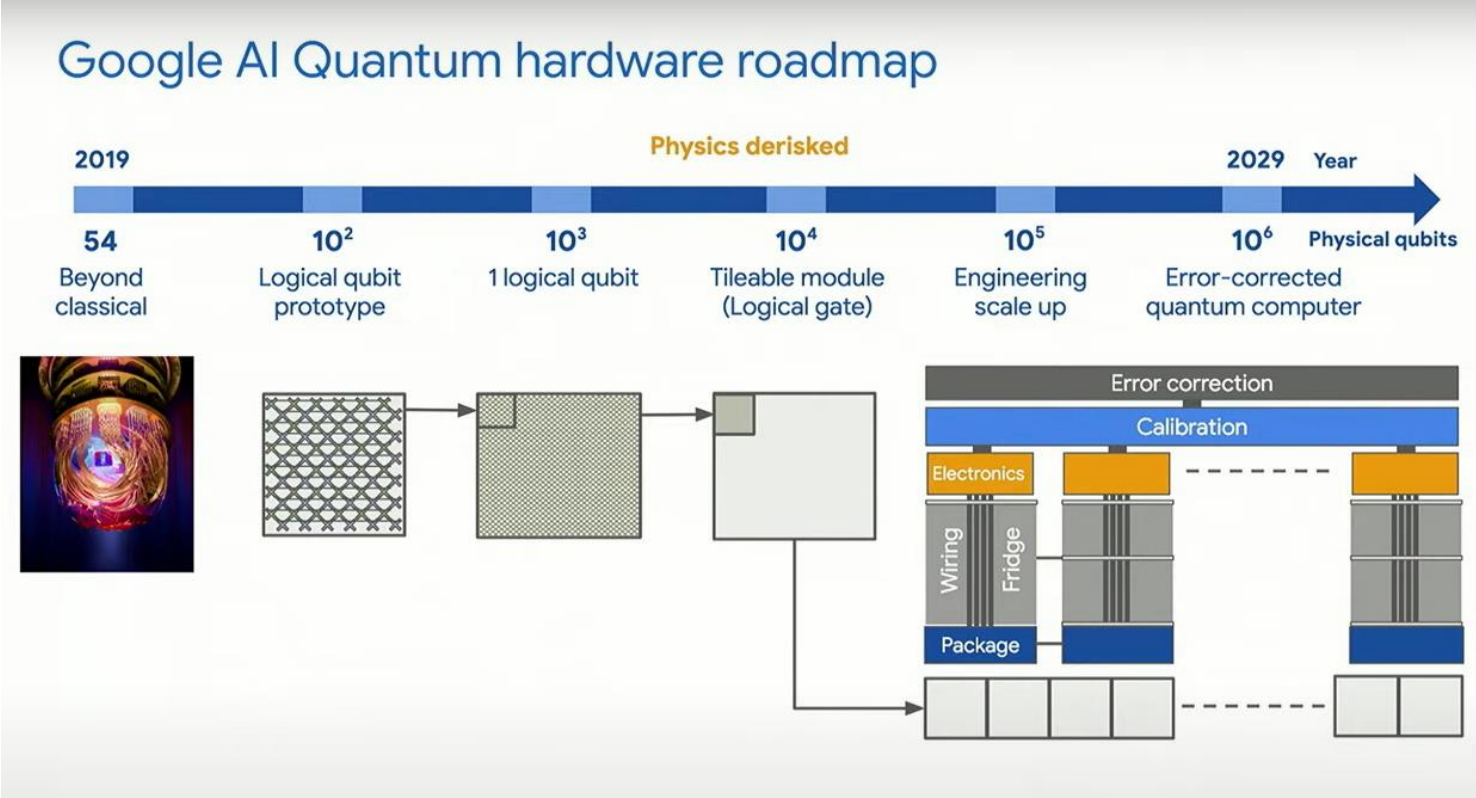
Google je jedna z ikonických technologických firem současnosti. Jejím počátkem je již legendární internetový vyhledávač. Prakticky všichni ho využívají, ať už hledají místo, kde se nají, co za telefon si koupí nebo získávají informace o prakticky čemkoliv.

Obrázek 9: Logo Google, zdroj: (18)

Jako počátek Google můžeme brát setkání obou zakladatelů Sergeye Brina a Larryho Page na Stanfordské univerzitě. Společně vytvořili vyhledávač, který se jmenoval BackRub. V roce 1998 získali investice a díky nim mohli založit společnost Google. Toto jméno vzniklo chybou přepsání matematického termínu googol, který znamená číslo jedna následované sto nulami. Postupem času získávali více finančních prostředků a jejich vyhledávač využívalo více a více lidí. V roce 2006 Google nakoupil Youtube. Gmail byl otevřen široké veřejnosti v beta verzi roku 2007. Mezi další služby, co Google nabízí patří například Google Books. Zde jsou veřejně dostupné oskenované knihy z knihoven a jiné digitální verze knih. Prohlížeč Google Chrome byl společností vyslán do světa v roce 2008. Na bázi tohoto prohlížeče v roce 2011 Google vydal operační systém pro počítače s názvem Chrome OS. Tento systém byl převážně distribuován v nevýkonných noteboocích z důvodu své nenáročnosti na hardware. V současnosti extrémně úspěšný systém mobilních zařízení Android byl poprvé vydán v chytrém telefonu T-Mobile G1. Poté následovala léta výroby telefonů Google Nexus partnerskými výrobci. Tato řada telefonů měla ukazovat jakým směrem se budou telefony s Androidem vyvíjet. Od roku 2015 je součástí holdingové společnosti Alphabet Inc. (17)

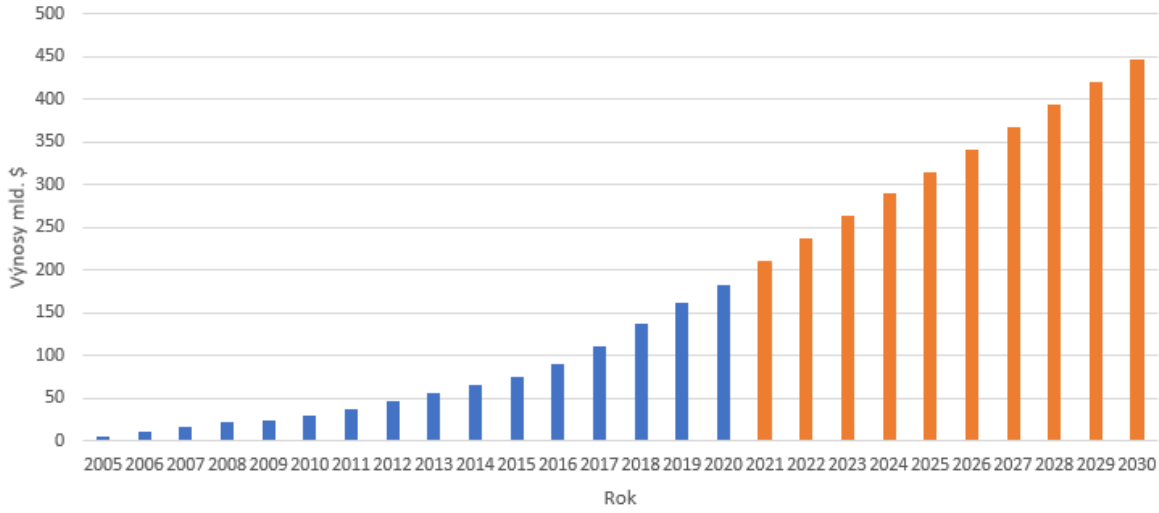
Společnost Google vytváří své vlastní kvantové počítače podobně jako je tomu u IBM. Jde o stejnou technologii supravodivých kvantových bitů. Jak již bylo zmíněno, tak v roce 2019 Google oznámil dosažení kvantové nadřazenosti viz. obrázky 3 a 4. (5) Toho bylo dosaženo za pomocí kvantového počítače Sycamore v Santa Barbaře. Zde sídlí tým Google Quantum AI, jehož součástí jsou výzkumné laboratoře, výrobní zařízení, kvantové datové centrum a zmíněný první kvantový počítačem, který dosáhl kvantové nadřazenosti. Kvantové počítače Googlu mají více jak deset tisíc součástek z čehož cryostat, lednice pro chlazení kvantových počítačů, je jen jedna z nich. Celý počítač má rozměr přibližně dvou metrů čtverečních. I přesto, že je kvantový procesor podobně velký jako procesor v našem stolním počítači, tak všechna elektronika, chlazení a stínění zabírají nejvíce prostoru v celém systému. (25)

Google jako většina společností následuje dobu NISQ éry kvantových počítačů. S tímto přístupem přichází určitá pozitiva, ale také problémy. Jako hlavní problém můžeme vnímat potřebu velkého množství qubitů ke korekci jiných kvantových bitů. Při přibližně 100 fyzických qubitů je možné studovat různé přístupy pro stavění logických kvantových bitů. Za pomocí logického qubitu je možné ukládat bezchybná kvantová data tak dlouho, abychom je mohli využít pro složité výpočty. Při 1000 fyzických qubitů je možné ukládat kvantová data po téměř rok. Dalším náročným krokem bude škálovatelnost na větší množství kvantových bitů. U 10 000 qubitů bude hlavním cílem jejich propojení. Tento krok bude vyžadovat velký pokrok u výroby a softwaru, který tento počítač bude řídit. Bude zapotřebí kolem 100 logických kvantových bitů k vytvoření prvního malého kvantového počítače s korekcí chyb. (26)



Obrázek 10: Plán vývoje kvantových počítačů Google, zdroj: (27)

Na obrázku 11 jsem vyobrazil vývoj výnosů pro holding Alphabet Inc., jehož je Google součástí. Vývoj výnosů každým rokem stoupá a dá se očekávat, že v tomto trendu bude nadále pokračovat.



Obrázek 11: Předpověď výnosů společnosti Alphabet Inc., zdroj: (15), vlastní zpracování

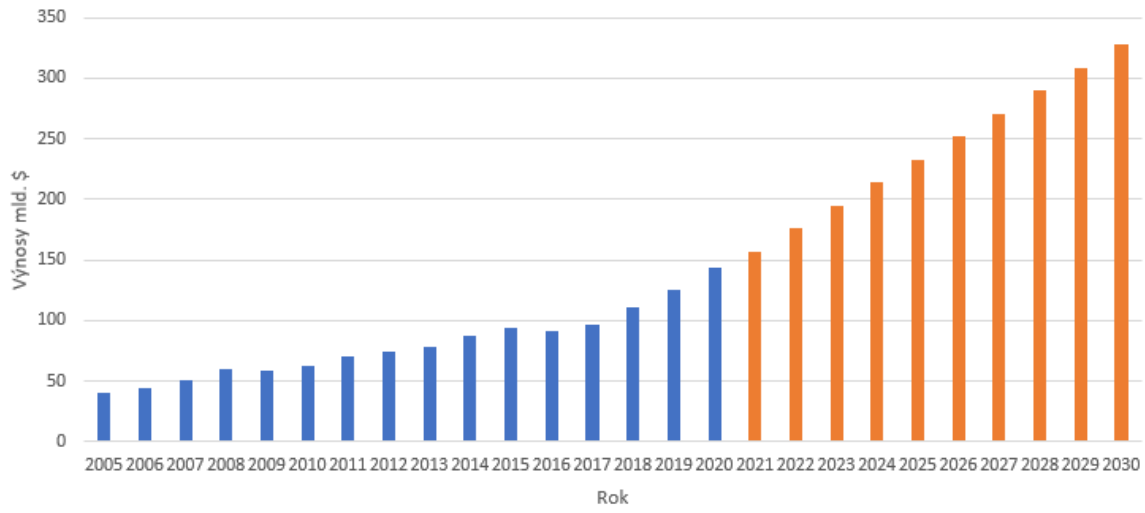
6.3 Microsoft

Příběh Microsoftu začíná, když Paul Allen a Bill Gates kontaktovali společnost MITS, která vyrobila mikropočítač Altair 8800. Nabídli této společnosti vyvinutí nového programovacího jazyka BASIC pro Altair. O osm týdnů později Gates a Allen demonstrovali BASIC společnosti MITS. Došlo k dohodě a produkt byl distribuován pod názvem Altair BASIC. To inspirovalo Gatese a Allena založit v roce 1975 svou vlastní společnost, kterou již známe pod názvem Microsoft. Prvním velkým úspěchem společnosti byl operační systém MS-DOS (Microsoft Disk Operating Systém) napsaný pro společnost IBM v roce 1981. Systém byl založen na základech operačního systému QDOS (Quick and Dirty Operating Systém). Gatesovi se podařilo vyjednat zachování vlastnického práva pro tento operační systém, šlo tedy o licencování MS-DOSu IBM. Díky tomuto vyjednání Gates pro Microsoft vydělal jmění a stala se z něj důležitá softwarová společnost. Roku 1983 uvedla na trh společnost svojí počítačovou myš.Ve stejném roce se jejich hlavním produktem stal operační systém Windows. Šlo o operační systém s již pokročilým grafickým a multitaskovým prostředím pro uživatele. V roce 1989 vydal Microsoft svůj softwarový balíček Office. S Windows 95 přišla možnost připojení k internetu a vestavěný webový prohlížeč Internet Explorer 1.0. V roce 2001 vydali svou první herní konzoli Xbox. V roce 2012 udělala společnost svůj první krok k výrobě vlastního výpočetního hardwaru v podobě tabletů Microsoft Surface. (28)

Obrázek 12: Logo Microsoftu, zdroj: (29)

Microsoft jako jediná z velkých společností zapojených do kvantového závodu sází na technologii topologických kvantových bitů. Jde o poměrně exotickou metodu vytvoření kvantového počítače. V roce 2018 vydal zaměstnanec Leo Kouwenhoven článek o nových důkazech o pozorování částice zvané Majorana fermion. (31) Microsoft měl v plánu využít tyto částice k vytvoření jejich topologického kvantového počítače. V tomto objevu tedy byla naděje, že by Microsoft měl šanci dohnat společnosti jako IBM a Google. Bohužel však Kouwenhoven v březnu roku 2021 vydal poznámku o stažení prohlášení o nalezení této částice. (32) Tato dramatická situace vede ke značnému zpomalení vývoje hardwaru jejich kvantového počítače. Microsoft vytvořil nový tým fyziků a matematiků za účelem vyladění teorie topologických qubitů. Prozatím stále jde o teorii a vypadá to tak, že na topologický kvantový počítač si ještě počkáme. (30)

I přesto, že vývoj jejich kvantového počítače je nám prakticky neznámý, tak na vývoji softwaru pro kvantové počítače pracuje Microsoft s velkou vervou. Nabízí kurzy zdarma pro všechny lidi, kteří se o softwarový vývoj u kvantových počítačů zajímají. Microsoft Learn je online platforma, kde můžete prohloubit své vědomosti o novějších technologiích podle vašeho tempa. Část tohoto programu je přímo věnována základům kvantových výpočtů, dále se věnuje identifikaci problematik, ve kterých je možné kvantové algoritmy řešit efektivněji a naučí vás, jak programovat přímo pro kvantové počítače. Quantum Katas je soubor tutoriálů a programovacích cvičení, která slouží k naučení kvantově výpočetních konceptů, operací a Q# programování (programovací jazyk pro kvantové algoritmy). (29)



Obrázek 13: Předpověď výnosů společnosti Microsoft, zdroj: (15), vlastní zpracování

6.4 Honeywell

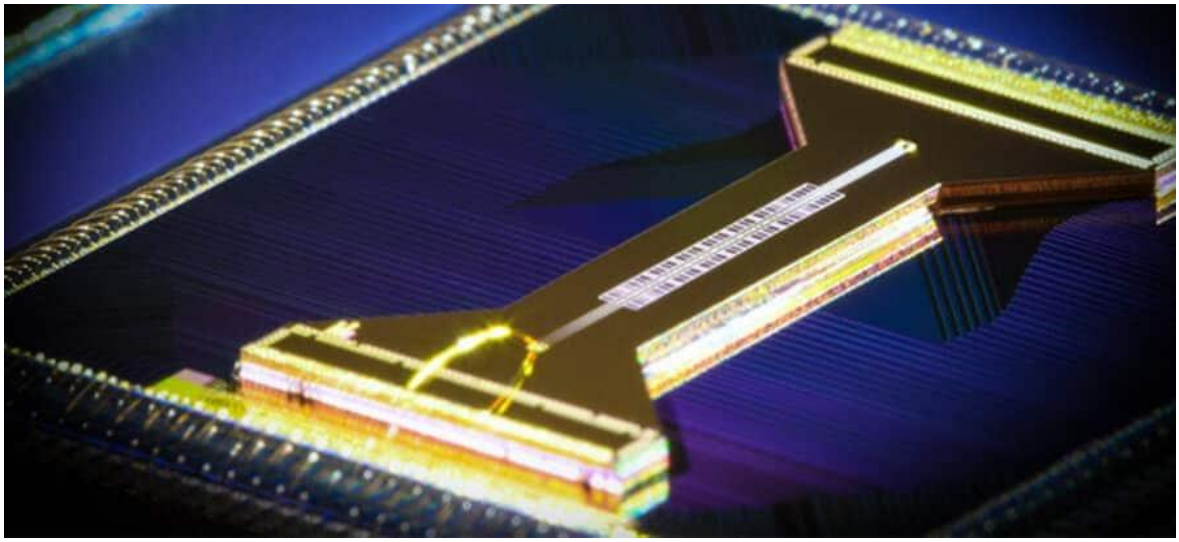
Jedná se o další firmu s dlouholetou tradicí založenou na inovacích. Jejich hlavním zaměřením je letectví, technologie ve stavebnictví, technologie materiálů a řešení produktivity a ochrany na pracovištích. Abychom lépe rozuměli, z jakého důvodu se Honeywell zapojuje do vývoje kvantových počítačů, tak si poukážeme na historické inovace a velké kroky pro tuto společnost. V roce 1885 vymyslel Albert Butz systém na automatický ohřev. Systém se skládal z termostatu, baterie a motoru. Tento motor by při nižší teplotě zvedl tlumení přístupu vzduchu k ohni a tím pádem zvýšil hoření a teplotu kamen. Jde tedy o počátky automatizace v domech, v dnešní době například klimatizovaný dům, který reaguje podle senzorů teploty. Během druhé světové války Honeywell vymyslel autopilota, který sloužil letcům. V šedesátých letech se firmě podařilo spolupracovat na vytvoření bezolovnatého benzínu. Olovnatý benzín byl v minulosti nejen nebezpečný pro prostředí, ale také pro lidi. Bezolovnatý benzín používáme i v současnosti. Ve stejném desetiletí Honeywell přišli s chemickým procesem pro výrobu biodegradabilního čistícího prostředku. V této době používá proces od této firmy více jak 85% světové produkce biodegradabilních čistících prostředků. V šedesátých letech také přišli se systémem pro vyhýbání se kolizím, který se využívá v letectví a přispěl tím k větší bezpečnosti létání. Podobně jako u společnosti IBM Honeywell přišel se svým čárovým kódem známým jako Code 39, a to v roce 1974. Na začátku třetího tisíciletí přišla firma s vylepšenou chladící kapalinou, která má nižší dopad na oteplování Země. (19)

Obrázek 14: Logo Honeywell, zdroj: (19)

Jedním z novějších zaměření Honeywellu jsou kvantové počítače. Podle historie je zřejmé, že hlavní přínos pro společnost měla automatizace a chemický vývoj. Jde přesně o ty oblasti, kde by kvantové počítače měly být klíčové. Není tedy asi překvapivé, že se právě tato firma pustila do jejich vývoje. Zajímavostí je, že jejich vstup do tohoto kvantového závodu byl velmi tichý. Jejich oznámení přišlo až s dobrými výsledky a plány na škálování jejich systému. Jejich kvantový počítač je založen na qubitech, které jsou vyrobeny uvězněním iontů.

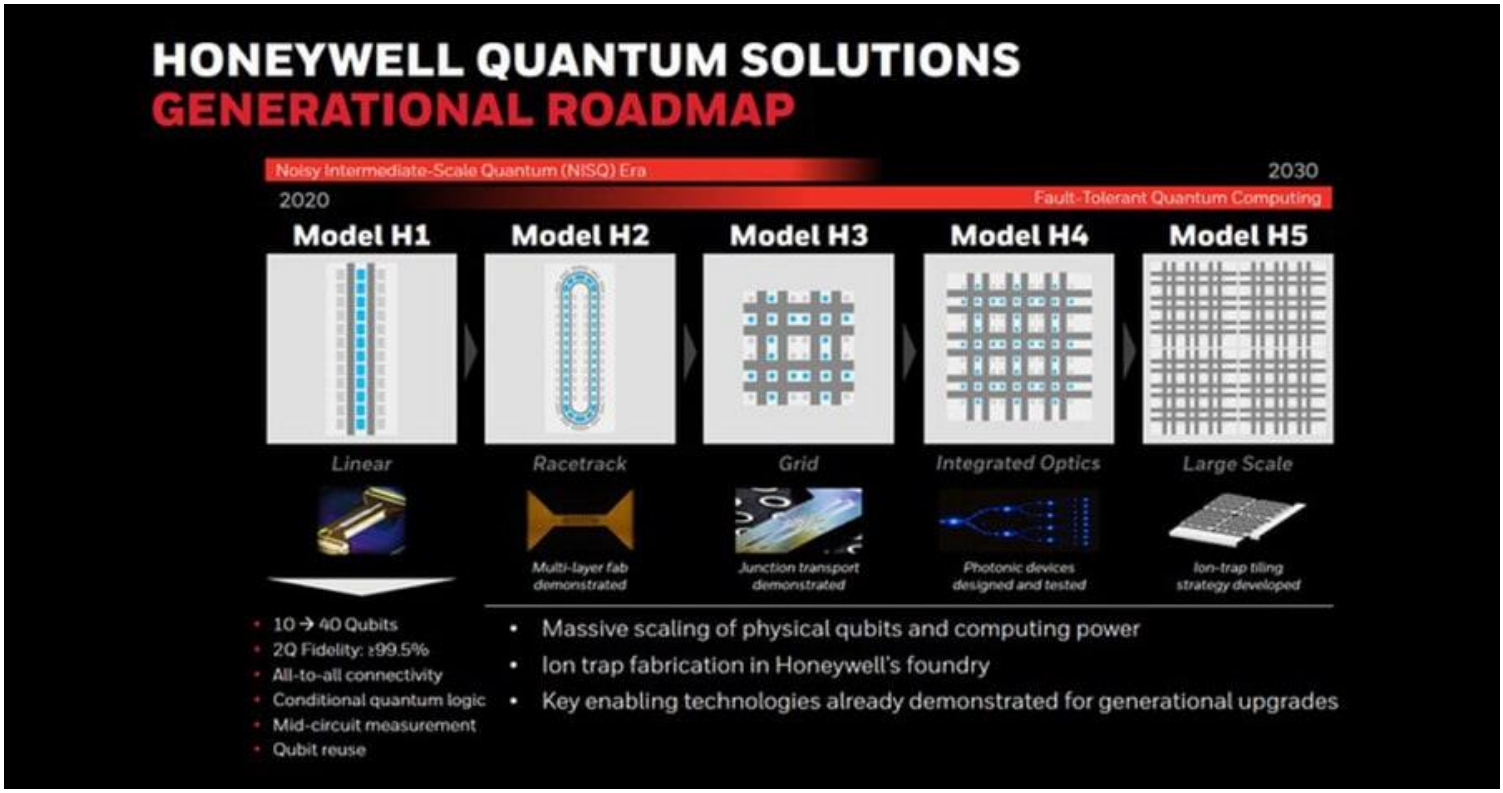
V červnu roku 2021 oznámil Honeywell fúzi své kvantové divize, která se zaměřuje na hardware kvantových počítačů se společnosti Cambridge Quantum Computing, která se zaměřuje na vývoj softwaru pro tento typ počítačů. Společnost demonstrovala možnosti korekce chybovosti u kvantových počítačů v reálném čase. Jako první společnost oznámila dosažení hodnoty 1024 kvantového objemu za pomocí 10 kvantových bitů ve svém počítači System Model H1. Jde o zdvojnásobení kvantového objemu oproti jejich předchozímu rekordu oznámenému v březnu 2021. (20) Společnost Cambridge Quantum Computing oznámila algoritmické pokroky, které

umožňují řešení komplexních optimalizačních problémů, za použití jen pár qubitů. Aplikování těchto nových poznatků povede Honeywell k dobrému postavení na trhu s optimalizací. (21) Honeywell již spolupracuje s dvěma velkými firmami na hledání řešení specifických problematik. Mezi tyto firmy patří BMW a Samsung. BMW v této spolupráci zkoumá optimalizování dodavatelského řetězce. (22) V případě Samsungu jde o simulování a testování nových materiálů pro potřeby akumulátorů. (23)



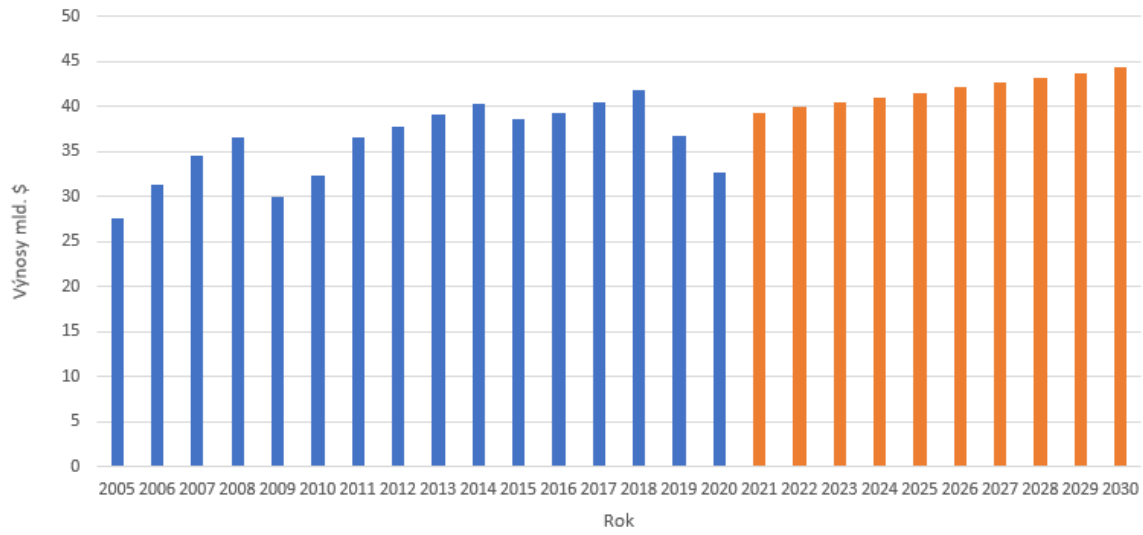
Obrázek 15: Honeywell System Model H1, zdroj: (24)

V roce 2020 Honeywell představil svůj plán generačního vývoje kvantových počítačů. Na obrázku 16 vidíme graficky vyobrazené představy do budoucna ohledně rozšiřování počtu qubitů v systému. Současný model procesoru H1 je lineární viz. obrázek 15, druhý model by měl mít tvar závodního oválu. V dalších modelech půjde o mřížky a o jejich škálovatelnost.



Obrázek 16: Plán vývoje kvantových počítačů Honeywell, zdroj: (24)

Na obrázku 17 vidíme vývoj výnosů společnosti. V posledních dvou letech se lehce výnosy propadly. Je však možné, že v roce 2020 byl dopad krize covid-19 byl pro tuto společnost poměrně znatelný. S budoucím vývojem je očekávaný návrat k postupným nárůstům výnosů. Tomu také napovídá předpověď na obrázku 20.

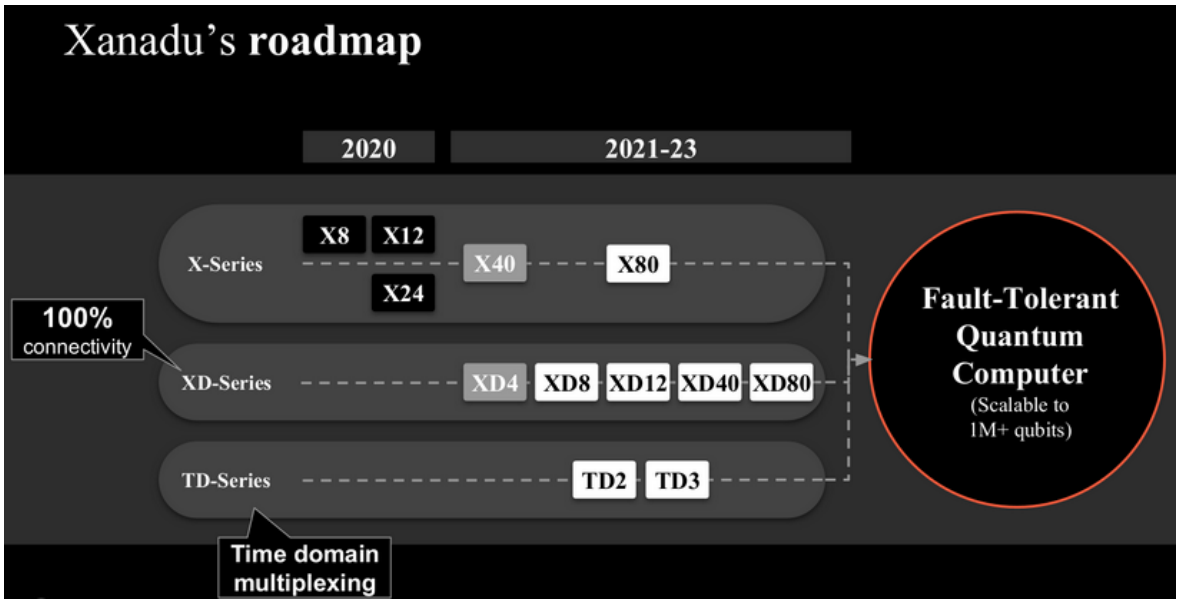


Obrázek 17: Předpověď výnosů společnosti Honeywell, zdroj: (15), vlastní zpracování

6.5 Xanadu

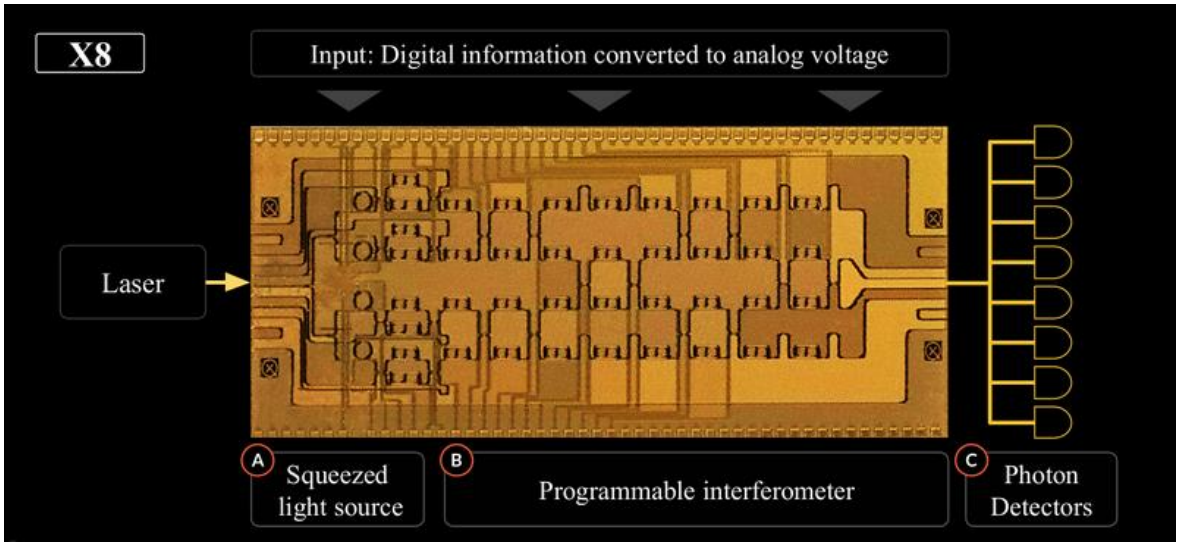
Společnost Xanadu byla založena roku 2016 a sídlí v Kanadě. Zadala si jako misi postavit kvantové počítače, které budou užitečné a dostupné všem lidem. Oproti předchozím společnostem se startupová společnost zaměřuje na vývoj kvantových počítačů na bázi fotonů. Xanadu se pro tento typ qubitů rozhodla z více důvodů. Možnost škálovatelnosti fotonických systémů je velmi dobrá. Jde o poměrně robustní qubity, což znamená, že jsou celkem odolné proti chybovosti a jsou flexibilní při navrhování korekce chyb. V neposlední řadě jde o praktičnost. Oproti nejrozšířenějším supravodivým qubitům mohou fotonické pracovat v pokojových teplotách. Dají se také snadno integrovat do již běžné telekomunikační infrastruktury, a díky tomu mohou být instalovány do běžných datových center. (33)

Obrázek 18: Logo Xanadu, zdroj: (33)



Obrázek 19: Plán vývoje kvantových počítačů Xanadu, zdroj: (34)

Na obrázku 19 vidíme plán vývoje kvantových procesorů společnosti Xanadu. Jejich plánem, je zdvojnásobit počet fotonických kvantových bitů každých šest až dvanáct měsíců. Na obrázku se jedná o sérii X (Obrázek 20). Za pomocí nanofotonických molekul vznikne XD série procesorů, která má dosáhnout stoprocentního propojení qubitů. TD série by měla sloužit k dosažení stovek a tisíců provázaných qubitů.



Obrázek 20: Fotonický kvantový procesor společnosti Xanadu, zdroj (34)

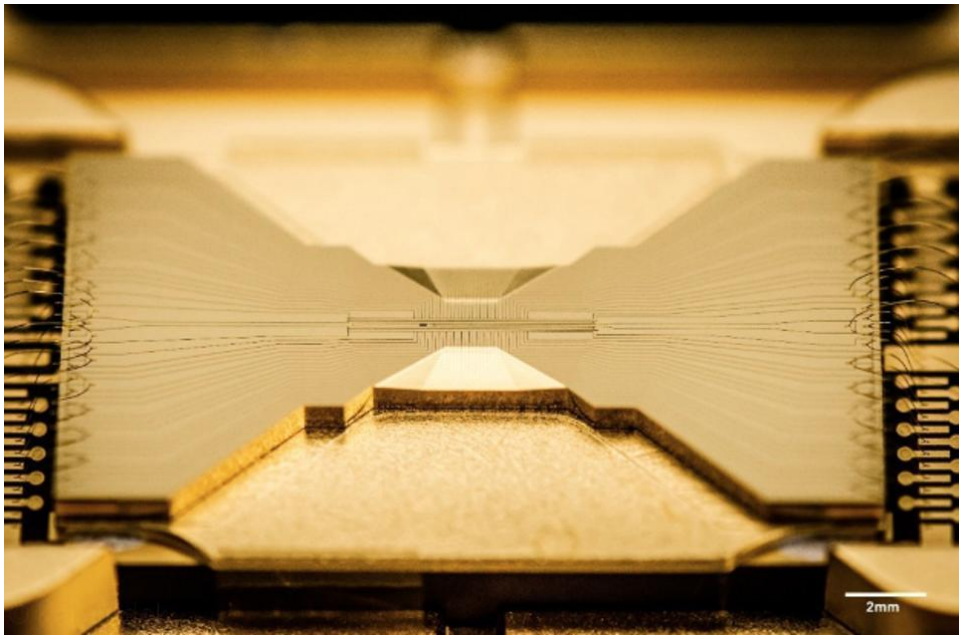
Osmi qubitový procesor Xanadu X8 vidíme s popisky na obrázku 20. Procesor využívá elektronické napětí k zakódování kvantového programu uživatele. Laser tuto informaci promění do programovatelně provázaného kvantového stavu za pomocí stlačených světelných zdrojů. Tato informace poté projde programovatelným interferometrem (jde o nástroj, ve kterém se k přesnému měření používá interference dvou paprsků světla) a nakonec je změřena fotonovými detektory. (34)

6.6 IonQ

Společnost byla založena v roce 2015 Chrisem Monroem a Jungsangem Kimem. Začali s dvěma miliony dolarů od společnosti New Enterprise Associateas a licencí technologie od univerzity Marylandu a Duku. Jejich cílem bylo přinést technologii uvězněného iontu na trh. Mezi jejich největší investory patří NEA, Samsung a Mukbadala. Oznámená partnerství jsou s Amazon Web Services, Microsoftem a Googlem, kteří dělají počítače IonQ dostupné v cloudu. (35)

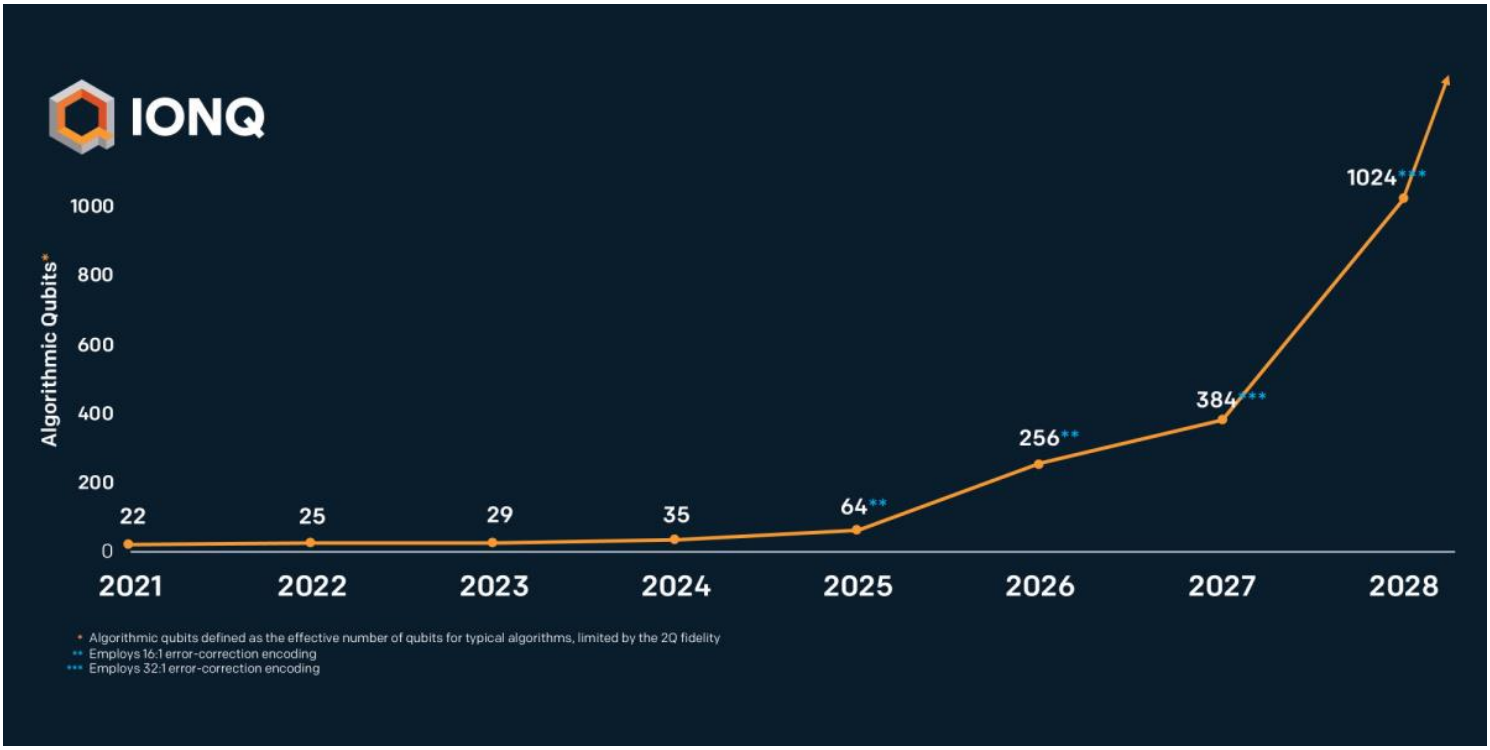
Obrázek 21: Logo společnosti IonQ, zdroj: (35)

IonQ v roce 2020 tvrdilo, že postavilo nejvýkonnější kvantový počítač na světě. Na svém kvantovém počítači s 32 qubity s očekávaným kvantový objemem přes čtyři miliony. Je to mnohonásobně vyšší číslo, než měl ve stejnou dobu oznámený objem 128 qubitový procesor společnosti Honeywell. I přesto, že jde jen o jednu z možností měření výkonu počítače, tak určitě lze přiznat, že jde o úctyhodný náskok. Další společnosti buďto kvantový objem neuváděli nebo nedosahovali ani jednoho tisíce, natož milionů. (36).



Obrázek 22: IonQ 32 qubitový procesor, zdroj: Kai Hudek, IonQ

Na obrázku 23 vidíme plán vývoje algoritmických qubitů. Jde o nové měřítko pro porovnání výkonu kvantových počítačů. Jde prakticky o největší číslo perfektních qubitů, které se dají využít pro typický kvantový program. Přitom se započítává korekce chybovosti a má přímý dopad na výsledný počet algoritmických kvantových bitů. IonQ počítá u 256 algoritmických qubitů s korekcí chybovosti 16:1 (šestnáct qubitů na jeden algoritmický) a u 1024 algoritmických počítá s korekcí 32:1. (37)



Obrázek 23: Plán vývoje kvantových počítačů IonQ, zdroj: (37)

6.7 Atom Computing

Misí společnosti je vytváření kvantových počítačů za použití individuálně kontrolovaných atomů. Atomy jsou podle společnosti perfektní přírodní kvantové bity a dají se ovládat opticky bez použití drátů. Jako další společnosti si zakládají na tvrzení, že jde o opravdu škálovatelný typ kvantového počítání. (38)

Obrázek 24: Logo společnosti Atom Computing, zdroj: (38)

Jejich prvním kvantovým počítačem je Phoenix, který byl světu představený v červenci roku 2021. Jde o první počítač se 100 atomovými qubity. Sice se jedná o první generaci takového systému, ale podle všeho vykazuje vysokou stabilitu. Jejich CTO říká, že koherence systému je na mnohem vyšší úrovni než ostatní komerčně dostupné kvantové systémy. Zapisují kvantovou informaci přímo do jádra daného atomu a ten nereaguje na okolní prostředí. Je sice náročné tuto informaci do jádra dostat, ale když už tam je, tak neuniká. (39) Díky takovému představení se Atom Computing prosadil a zajisté překvapil velké společnosti. Stále však jde o počátky společnosti a musíme se nechat překvapit, zda přijdou s dalšími velkými zprávami.

6.8 Další společnosti

Vypsané společnosti v předchozích kapitolách však zdaleka nejsou všechny firmy, co se vývojem hardwaru kvantových počítačů zabývají. Je ale rozhodně vidět, že Severní Amerika je v popředí komerčního vývoje.

6.8.1 Intel

Intel jako jedna ze dvou největších společností se zaměřením na výrobu procesorů pro klasické počítače je jeden z velkých hráčů kvantové soutěže. Mezi více popsanými společnostmi není uveden, protože se o Intelu moc nemluví, alespoň z hlediska vývoje procesorů pro kvantové počítače. V roce 2020 však představila společnost svůj nový kvantový procesor jménem Horse Ridge 2. (40)

6.8.2 D-Wave

D-Wave nabízí kvantové počítače převážně pro praktické využití. Jejich kvantový počítač D-Wave Advantage dosahuje více jak 5000 qubitů s vysokou propojeností těchto kvantových bitů. Nejde však o počítač, který by dokázal tyto qubity využít k logickým operacím. D-Wave počítače slouží převážně k optimalizacím.

6.8.3 Amazon Web Services (AWS)

AWS nabízí službu Amazon Braket. Jde o službu, která napomáhá vývojářům začít s technologií pro urychlení výzkumu a objevování. Nabízí vývojové prostředí, ve kterém se dají zkoumat a vytvářet kvantové algoritmy, testovat je za pomocí simulátorů kvantových obvodů a spouštět tyto algoritmy na různých kvantových hardwarových technologiích. Mezi ně patří počítače od D-Wave, IonQ a Rigetti. (41)

6.8.4 Cold Quanta

Cold Quanta v červenci 2021 oznámila 100 qubitový kvantový počítač Hilbert se svou technologií studeného atomu. Zatím nejde o přístupný počítač, ale očekává se, že bude později tento rok. Tento úspěch demonstruje potenciál rychlého škálování jejich počítače. (42)

6.8.5 Rigetti

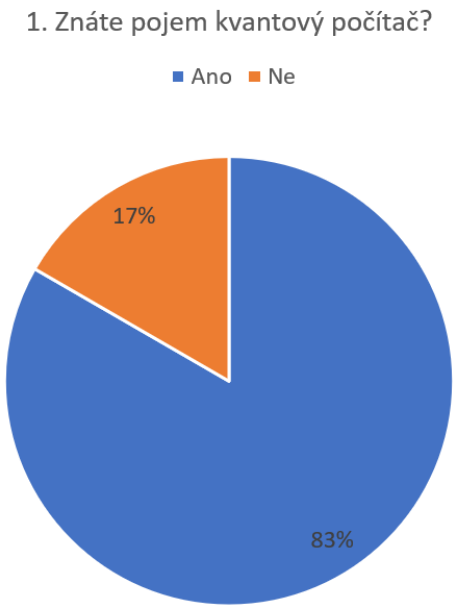
V červnu roku 2021 společnost Rigetti, která vytváří kvantové počítače na bázi supravodivé drátové smyčky spojené s rezonátorem (transmon), přišla s řešením pro škálování jejich počítače. Využije metody modularity. Sice má Riggeti zatím jen 31 qubitový systém, tak doufá, že za pomocí modulární výroby bude možné tento počet navýšit. (43)

6.8.6 PsiQuantum

Společnost si zakládá na realizaci a postavení prvního užitečného kvantového počítače. Počítá s tím, že k jeho realizaci bude potřeba více jak milion qubitů. PsiQuantum vkládá důvěru ve fotonické qubity. Nejde jim tedy o pomalé kroky a posuny jako v případě některých větších společností, ale jen o finální produkt jako takový. Chtěli by dosáhnout svého cíle do roku 2025. (44)

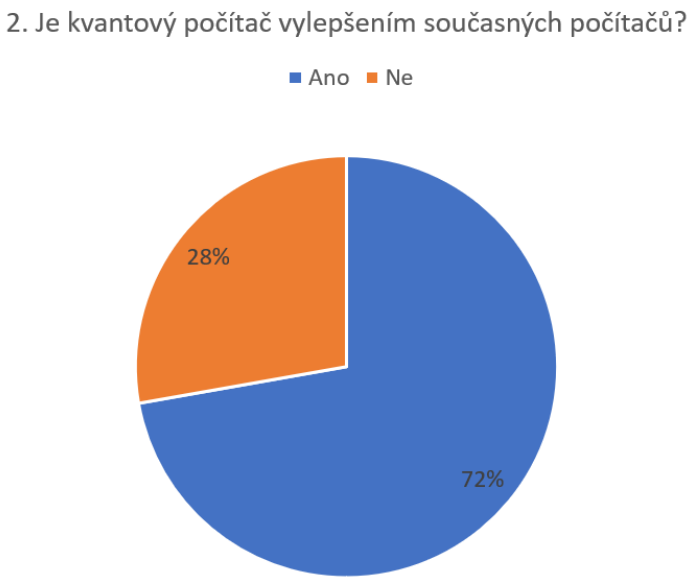
7 DOTAZNÍK

Za pomocí dotazníku jsem analyzoval, zda studenti technického oboru tuší, co to je kvantový počítač. V dotazníku se schválně objevují otázky, které by mohly být brány jako chytáky. Jsou zde z toho důvodu, aby se nejednalo o falešně pozitivní odpovědi. Dotazník vyplnilo osmnáct studentů. Cílem dotazníku je zjištění jaké informace by neměli chybět při představování kvantových počítačů, a také zda jsou studenti připraveni, alespoň základními informacemi na jejich příchod.



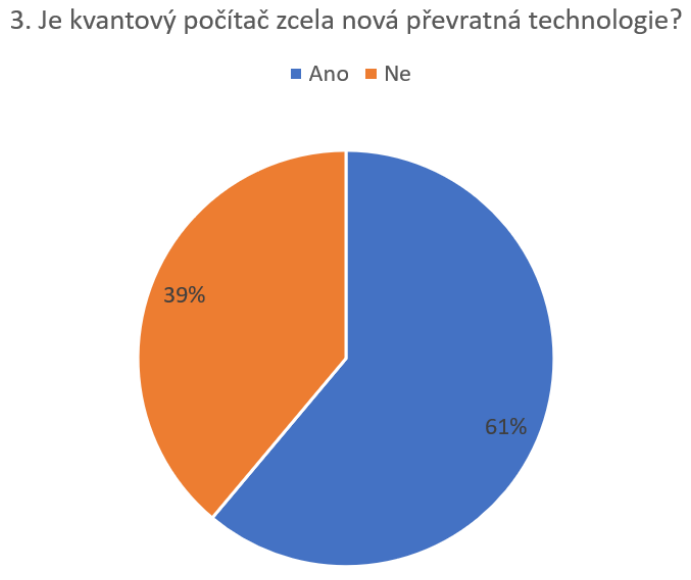
Obrázek 25: Otázka 1: Znáte pojem kvantový počítač?

První otázka zjistila, že se většina studentů s pojmem kvantový počítač již setkala. V dalších otázkách bude vidět do jaké hloubky tento pojem znají.



Obrázek 26: Otázka 2: Je kvantový počítač vylepšením současných počítačů?

Mnoho lidí, jak je vidět již podle odpovědí by řeklo, že kvantový počítač je lepší verze toho klasického. Bohužel tomu tak úplně není. Kvantový počítač, i přesto, že si vypůjčuje některé z postupů počítače klasického, není vylepšením. Jde o úplně novou technologii, která je postavena na jiných základech a principech. Podle všech informací také kvantové počítače nenahradí již zažité počítače.



Obrázek 27: Otázka 3: Je kvantový počítač zcela nová převratná technologie?

Ano jedná se o novou převratnou technologii. V praxi se začala využívat před pár lety, ale její plné využití nás zatím čeká.

Obrázek 28: Otázka 4: Znáte firmy, které kvantové počítače vyvíjejí nebo komerčně nabízejí?

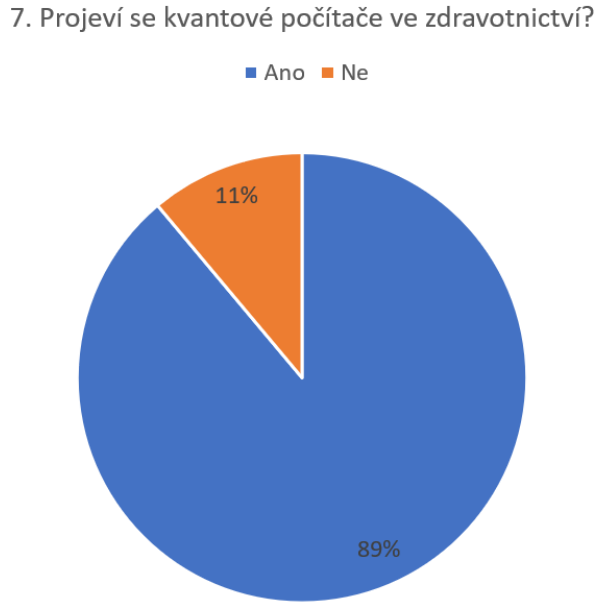
Není vůbec překvapující, že přehled o firmách, které vyrábí kvantové počítače studenti nemají. Žádnou propagaci od nich neuvidíte. Jedná se většinou jen o blízkou spolupráci mezi velkými společnostmi při prodeji těchto počítačů.

Obrázek 29: Otázka 5: Je rychlost výpočtu kvantových počítačů nekonečná?

V této falešně pozitivní otázce se studenti většinou nezmýlili. I přesto, že kvantové počítače přinesou v určitých užitích mnohonásobně vyšší výkon, tak rychlost výpočtu nekonečná nemůže být.

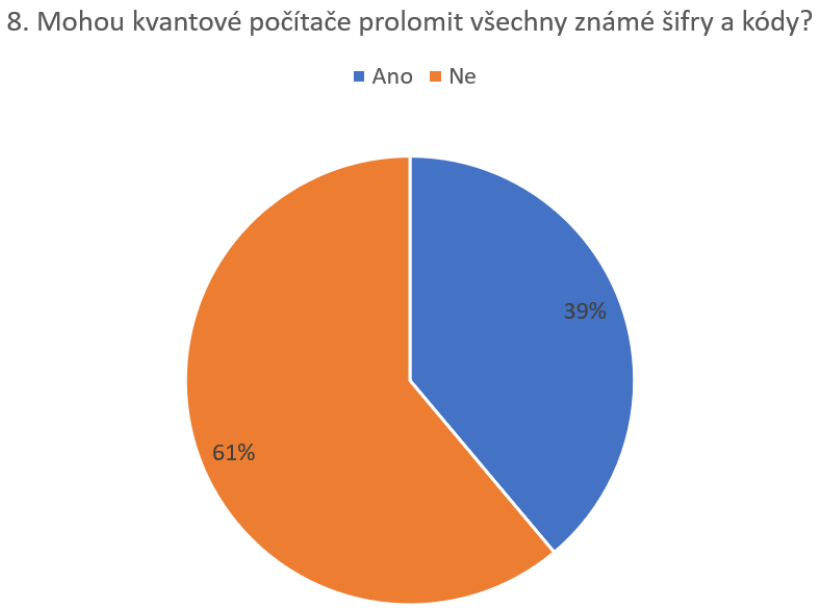
Obrázek 30: Otázka 6: Převyšuje rychlost výpočtu kvantových počítačů všechny známé superpočítače?

Ano ve specifických úkonech jsou kvantové počítače o mnoho rychlejší než superpočítače. S vylepšováním kvantových počítačů můžeme být připraveni na úplně jiné možnosti výpočtů.



Obrázek 31: Otázka 7: Projeví se kvantové počítače ve zdravotnictví?

Přesně tak, a již v současnosti se projevují při vývoji léků a vakcín.



Obrázek 32: Otázka 8: Mohou kvantové počítače prolomit všechny známé šifry a kódy?

Technicky tomu tak je. Ale některé jen v nereálném časovém horizontu

8 PROGNOSTICKÉ METODY

Někým je prognostika považována za vědní obor, jinými není. Tento spor ve vnímání prognostiky však nemá dopad na její důležitou roli při nahlížení do budoucnosti. S její pomocí se můžeme lépe rozhodovat, jak naložíme například s prostředky na vývoj, jaká je nejlepší cesta podnikání nebo jak bychom se měli připravit na možnou budoucnost.

8.1 Kvalitativní metody

U kvalitativních metod využíváme informací, názorů odborníků a osobností v oblasti, kterou zkoumáme. (10) Jde spíše o subjektivní a úvahové metody. Využíváme je v případech, kdy nedokážeme sledované vlivy a veličiny, které působí na jejich vývoj, kvantifikovat. (11)

8.1.1 Brainstorming

Jde o metodu, u které se snažíme vygenerovat větší množství nápadů na zvolené téma. Toho dosahujeme za pomocí týmové spolupráce. Běžné využití je v managementu, podnikání a v prognostice. Brainstorming většinou probíhá ve skupině, která nepřesahuje dvacet lidí, jde o diskuzi, která se běžně řídí následujícími pravidly:

- Experti by měli mít podobnou úroveň vzdělání a podobné společenské postavení
- Diskuze se odehrává přátelsky, v neformálním, optimistickém a klidném prostředí
- Je důležitá formulace otázek a mělo by se vyhýbat skepticismu
- Nápady se anonymně zaznamenávají
- Finální formulace a hodnocení provádí jiná skupina odborníků podle zaznamenaných nápadů (10)

8.1.2 Panel expertů

Jde o metodu, u které experti analyzují velké množství dat během delšího časového úseku (3-24 měsíců). Jako výstup je finální zpráva, která vyobrazuje možnosti dalšího vývoje zkoumaného problému. Jde o časově i finančně náročnou metodu.

8.1.3 Metoda Delphi

Jde o časové náročnou metodu založenou na anonymním více kolovém odhadování expertů. Jde zároveň o metodu využívanou k řízení projektů a jejich dílčích částí. Metoda patří také k nejpoužívanějším metodám kvalitativní analýzy rizik, k metodám expertního odhadování. Slouží k vytváření originálních myšlenek podobně jako je tomu u metody brainstormingu. Podle literatury je vhodná ke stanovování plánovaných hodnot projektů. Podobně jako u metody brainstormingu spolupracují experti, avšak za pomocí informačních technologií spolu komunikují anonymně, čímž se zamezuje psychologickým bariérám při přímém kontaktu. Za pomocí sbíraných dat se ve více kolech názory expertů mění a dostávají se k lepším formulacím prognózy.

Průběh metody:

1. Sestavení komise (3-5 členů)
2. Přesné definování problému
3. Získání vhodných expertů
4. Následují 2 až 3 kola dotazníků (v intervalech jednoho až dvou měsíců), které jsou zasílány expertům. Po každém dotazníku se vyhodnocují podobné a jiné názory

odborníků. Experti by měli mít možnost posoudit názory jiných odborníků a přehodnotit své stanovisko. Jde o snahu získat shodu názorů těchto expertů

5. Zpracování výsledného odhadu v konečné zprávě (10)

8.1.4 Metoda analogie

Metoda analogie pracuje na bázi podobnosti znaků, vývoje a struktury. Cílem je využití již proběhlých událostí u podobného případu a promítnutí na případ právě řešený. Odhadujeme tedy podobný výsledek u obou případů. Jde o náročnou metodu z časového hlediska i z hlediska nároků na experta. Využití je vhodné s expertovou opatrností v těchto příkladech:

- Hledání analogie prognózovaného procesu s procesem dalším, který již v minulosti proběhl (analogie historická)
- Hledání analogie u vývoje technicko-ekonomického systému s vývojem biologického
- Při určování vývoje trendu, u kterého neznáme vhodnou metodu podle vývoje známého trendu, kde prognózu známe (10)

8.2 Kvantitativní metody

8.2.1 Časové řady

Jde o hlavní kvantitativní metodu, s kterou se můžeme setkávat. Jde o po sobě následující hodnoty v čase, podle kterých je možné predikovat jejich další vývoj. Časové řady můžeme rozdělovat na deterministické a stochastické.

- Deterministické časové řady jsou bez náhodného prvku. Hodnoty je možné přesně předpovídat při znalosti dané analytické funkce, která je vytváří.
- Stochastické časové řady jsou naopak řady s náhodným prvkem. Nelze je tedy přesně popsat pomocí matematického vztahu s konstantními funkčními parametry.

Podle této teorie je vidět, že naprostá většina ekonomických časových řad jsou stochastickými. Dále lze dělit časové řady na absolutní (neodvozené) a relativní (odvozené) ukazatele.

- Absolutní ukazatele jsou dány pozorováním nebo měřením.
- Relativní ukazatele jsou nějakým způsobem přeměněny nebo odvozeny od ukazatelů absolutních.

Další rozdělení je na okamžikové a intervalové časové řady.

- Okamžikové časové řady se vztahují ke konkrétnímu okamžiku.
- Intervalové se vztahují k určitému časovému úseku.

Okamžikové řady tedy měří jen stavové hodnoty spojené s určitým časovým bodem a intervalové měří tokové hodnoty v určitém časovém rozpětí. Proto se dále časové řady rozdělují na dlouhodobé a krátkodobé.

- Jako dlouhodobé jsou řazeny ty časové řady, u kterých jsou hodnoty sledovány v ročních a delších časových intervalech.
- Krátkodobé jsou časové řady, kde jsou hodnoty sledovány v kratších intervalech, než je jeden rok.

Ještě dělíme časové řady podle pravidelnosti zaznamenaných údajů jako ekvidistantní a neekvidistantní.

- Ekvidistantní jsou ty časové řady, které mají konstantní časovou délku mezi zaznamenanými hodnotami.
- Neekvidistantní jsou ty s proměnlivou časovou délkou mezi zaznamenanými hodnotami. (10)

9 ANALÝZA PROSTŘEDÍ

V představení společností, o kterých je velmi slyšet byly obsaženy téměř jen Americké společnosti. Není to překvapivé, Američané jsou v historii vývoje moderních technologií na špici. Soupeří však s Čínou, která investuje masivní částky právě do stejného vývoje. Je vidět, že si rozhodně nechtějí nechat ujet vlak. Mají v plánu vést tento posun do nové éry výpočetní techniky. Je však nutné mít i přehled o tom, co se děje v jiných částech světa. Vybral jsem země a společnosti, co se nejvíce podílí na vývoje technologie kvantových počítačů.

Trh kvantových počítačů je v roce 2021 ohodnocen na 472 milionů dolarů a podle odhadů by měl dosáhnout hodnoty 1.7 miliardy dolarů v roce 2026 se složenou roční mírou růstu 30.2 procent. (59)

9.1 Spojené státy americké

V roce 2019 vláda spojených států založila instituci National Quantum Initiative, která se zabývá stavbou infrastruktury pro budoucnost kvantových počítačů. NQI spolupracuje se školami, aby nabízeli vzdělání spojené s kvantovými počítači. Spolupracuje s americkými společnostmi, které na vývoji kvantových počítačů přímo podílí. Vláda uvolní 1.2 miliardy dolarů během pěti let na podporu kvantového vývoje. Ministerstvo energetiky podpoří dalšími 80 miliony dolarů. V roce 2020 oznámil Úřad pro vědu a technologickou politiku Bílého domu, Národní vědecká nadace a ministerstvo energetiky fond 1 miliardy dolarů k zřízení 12-ti výzkumných center pro kvantovou informační vědu a center pro umělou inteligenci. (59) Se společnostmi jako IBM, Google, Honeywell, Microsoft, Ionq a mnoho dalšími patří Spojené státy k favoritům tohoto kvantového závodu.

9.2 Čína

V roce 2017 vyhlásil čínský prezident Xi Jinping, že Čína musí vyvstat jako globální vůdce inovací do roku 2035. Čína provedla velké investice do vývoje kvantových počítačů. Čína buduje národní laboratoř kvantové informační vědy, která je financována 1 miliardou dolarů. (59) V roce 2016 se Číně podařila kvantová komunikace za pomocí QKD. Jako prvním se jim podařilo dosáhnout kvantové komunikace a propojit více jak 150 lidi. (57) V roce 2020 se čínským specialistům povedlo vzorkovat boson fotonu za pomocí jejích 76 qubitového kvantového počítače. Tím prokázali kvantovou nadvládu. Úkon vzorkování bosonu by klasickému superpočítači trvalo 2.5 miliardy let. Jejich kvantový fotonový počítač to dokázal jen za 200 sekund. V současnosti jde asi o nejvýkonnější kvantový počítač na takovou úlohu. (60) Dále se čínským vědcům podařilo spojit

mezi satelitem Micius a třemi pozemními stanicemi za pomocí QKD. Jde o další masivní úspěch čínských vědců. (61) Čínský nejvýkonnější supravodivý kvantový procesor má v současnosti 66 qubitů. Výkonem překoná procesor Sycamore od Googlu a mnoho dalších. S největší pravděpodobností patří mezi nejvýkonnější na světě. (62) V Číně nejde jen o vývoj placený státem, ale najdeme zde i řadu komerčních společností, které se do vývoje kvantových počítačů také zapojují. Mezi tyto společnosti patří Origin Quantum nebo QuDoor. V převážně softwarové sféře je například Alibaba Cloud, Huawei Cloud nebo Baidu research.

9.3 Kanada

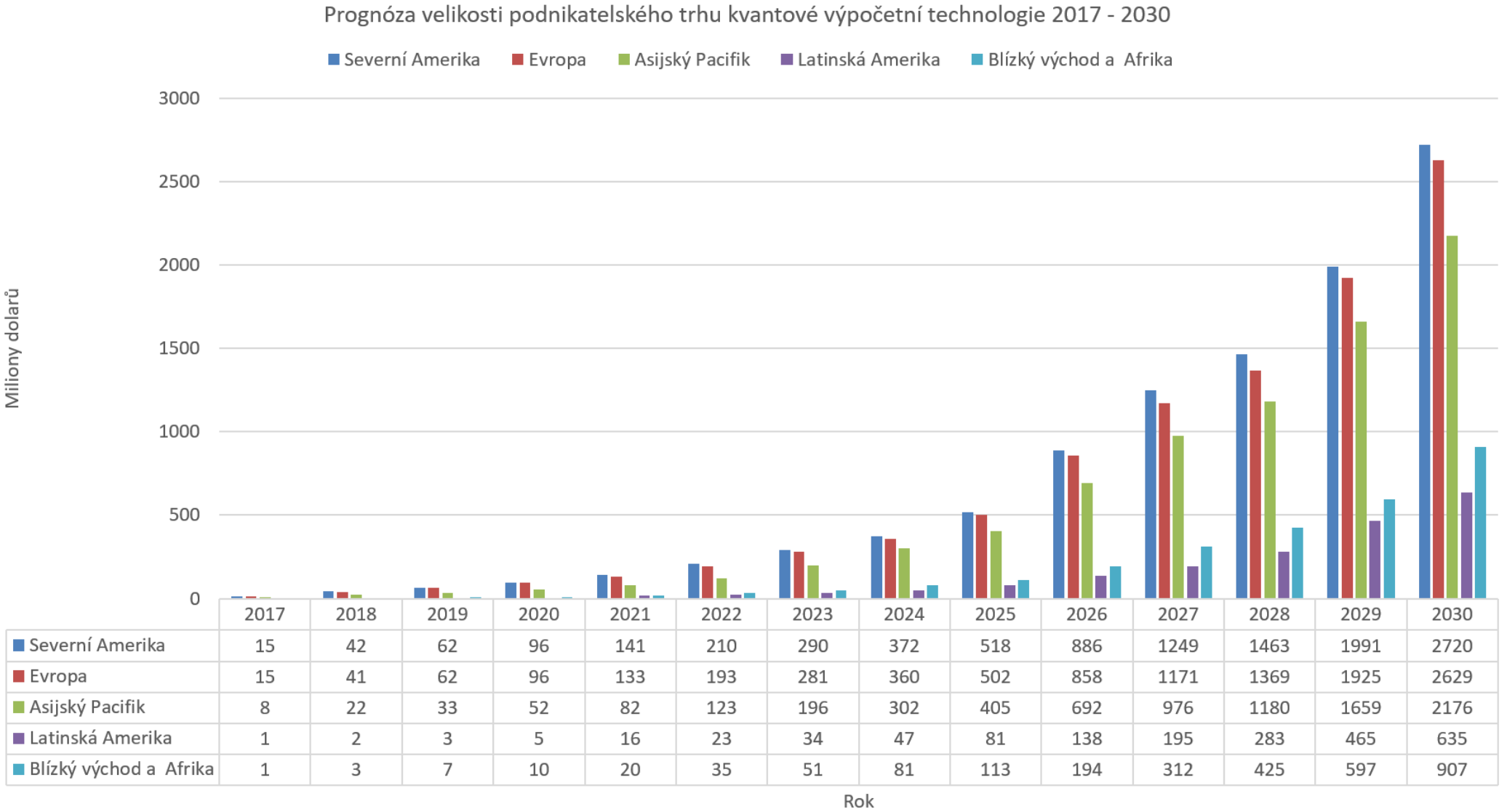
Kanada za posledních 10 let investovala do kvantových počítačů 1 miliardu dolarů. V Kanadě najdeme mnoho talentovaných expertů na vývoj kvantových systémů. (59) Společnost D-Wave sídlí v Kanadě, jak už bylo řečeno se zabývá kvantovými annealery. Jde však o jednu z komerčně neúspěšnějších firem v kvantové sféře. Vydávají se sice jinou cestou, ale v současné době dávají kvantové annealery větší smysl pro praktické využití. Další již zmíněnou společností je Xanadu, která vyvíjí kvantové počítače na bázi fotonů.

9.4 Evropa

Evropská unie hodlá soupeřit za pomocí projektu, který začal v roce 2018 a má za plán postavit 100 qubitový kvantový počítač. Tento počítač bude přístupný v superpočítačovém centru Jülich. Prozatím dosáhli 2 qubitového systému. (63) Finské VTT (finské technické výzkumné středisko) a IQM se spojily k tomu, aby pro Finsko vytvořily 50 qubitový kvantový počítač do roku 2024. Finská vláda do tohoto projektu vložila 20.7 milionu eur. (64) Společnosti v Evropě, o kterých se mluví ve spojení s kvantovými počítači jsou Accenture (Irsko), Cambridge Quantum Computing (Spojené království), Alpine Quantum Technologies (Rakousko) a Airbus (Francie).

9.5 Japonsko

Japonsko hodlá v následujících deseti letech investovat 270 milionů dolarů do technologie kvantových počítačů. Dále usilovně podporuje jejich výzkum a vývoj. Podle médií má Japonské snahu vybudovat plnohodnotné kvantové počítače do roku 2039 (59) Mezi známé společnosti, co se na vývoji kvantových počítačů podílí je Fujitsu, Hitachi, Mitsubishi, NEC a Toshiba.

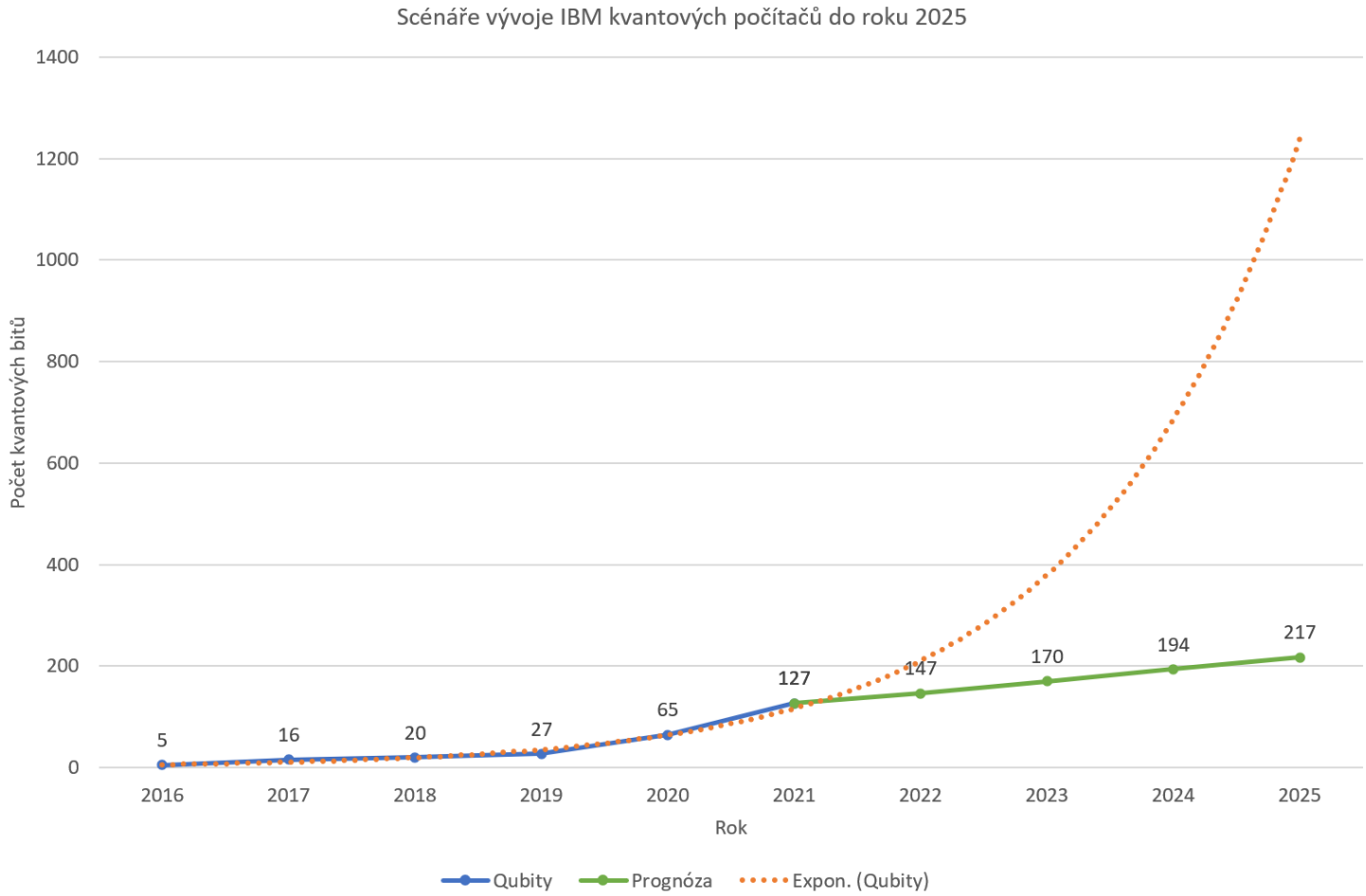


	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Severní Amerika	15	42	62	96	141	210	290	372	518	886	1249	1463	1991	2720
Evropa	15	41	62	96	133	193	281	360	502	858	1171	1369	1925	2629
Asijský Pacifik	8	22	33	52	82	123	196	302	405	692	976	1180	1659	2176
Latinská Amerika	1	2	3	5	16	23	34	47	81	138	195	283	465	635
Blízký východ a Afrika	1	3	7	10	20	35	51	81	113	194	312	425	597	907

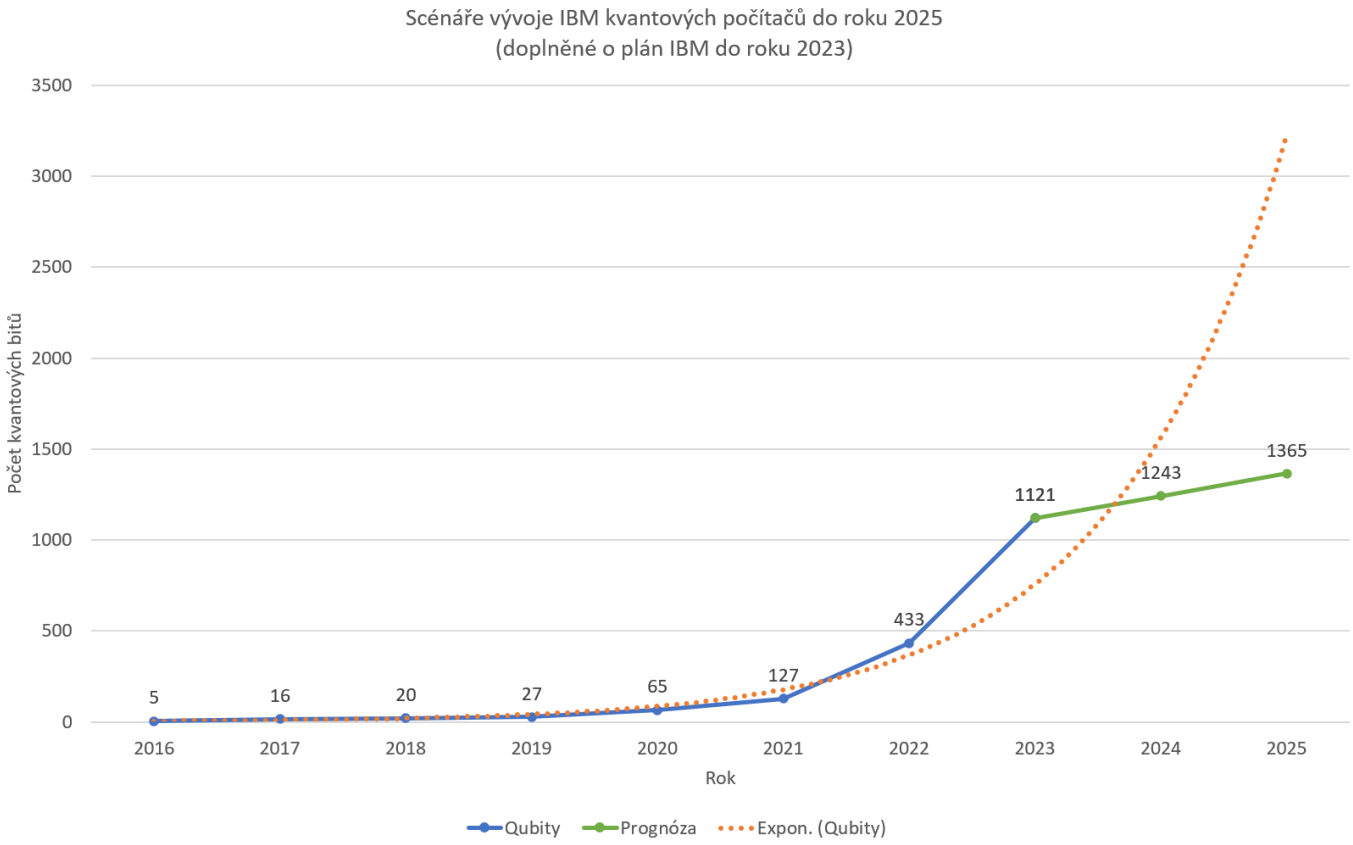
Obrázek 33: Prognóza velikosti podnikatelského trhu kvantové výpočetní technologie 2017 – 2030, zdroj: (68)

10 PROGNÓZA VÝVOJE

V této kapitole budu prognózovat vývoj kvantových počítačů do ne tak vzdálené budoucnosti. K této prognóze jsem došel za pomocí výběru nejsilnější společnosti IBM. Jejich historie ve vývoji a množství investovaných peněz a také díky tomu, že v době psaní vlastní nejvýkonnější kvantový počítač. Zbylé společnosti bylo bohužel nutno vyřadit z důvodu nedostatku dat nebo kvůli jen jednotlivým kvantovým strojům. Jde tedy o supravodivý kvantový počítač, který je založený na korekci chyb. Byla zadána data v podobě počtu kvantových bitů na předchozích modelech kvantových počítačů IBM společně s rokem jejich představení. Jde o vlastní prognózu stochastické časové řady s absolutními ukazateli. Na obrázku 34 vyjadřuje zelená křivka růst qubitů za nepříznivých podmínek. Oranžová exponenciální naopak vyjadřuje optimistický růst. Ale zdaleka nejde o tak optimistický růst, jak to může vypadat. Už jen díky povaze kvantových počítačů je růst exponenciální a tato prognóza je i podporována velmi optimistickým plánem IBM, který můžeme vidět na obrázku číslo 35. Na něm jsou přidány dva předpokládané kvantové počítače, na kterých IBM již pracuje. V běžných případech by bylo nejbezpečnější prognózou udělat průměr mezi lineární a exponenciální regresí. Za pomocí prognózování metodou analogie je možné porovnat vývoj kvantových počítačů s těmi klasickými. Jediným rozdílem je zrychlený vývoj počítačů kvantových.



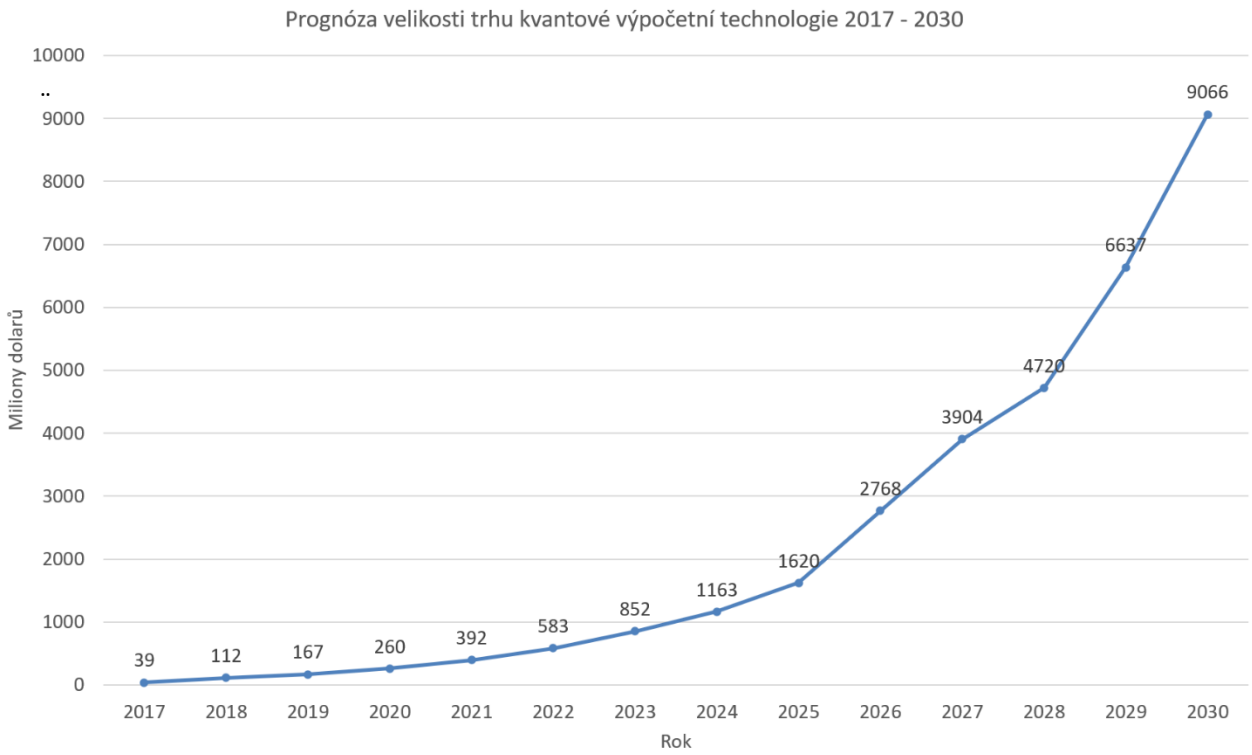
Obrázek 34: Scénáře vývoje IBM kvantových počítačů do roku 2025, zdroj: (16), (67), vlastní zpracování



Obrázek 35: Scénáře vývoje IBM kvantových počítačů do roku 2025, zdroj: (16, (67)

(doplněné o plán do roku 2023)

Obrázek 35 je prodloužený o 433 a 1121 qubitové počítače, které má IBM v plánu představit v následujících letech.



Obrázek 36: Prognóza velikosti trhu kvantové výpočetní technologie 2017 – 2030, zdroj: (66)

Obrázek 36 je prognózou velikosti trhu v milionech dolarů.

Předpověď rozdělím na tři různé časové úseky. První úsek je o 4 roky později v roce 2025, dále půjde o rok 2030 a poté popíšu rok 2040. Tento popis by měl poukázat na to, jaký dopad by mohly mít kvantové počítače v průběhu let.

10.1 Předpověď 2025

V roce 2025 mají společnosti 500 qubitové supravodivé procesory. Propojení mezi qubity je přibližně 40 %. Kvantové počítače na bázi iontových pastí dosahují přibližně 300 kvantových bitů a dosahují 60 % propojenosti mezi qubity. Fotonové procesory dosahují asi 500 qubitů s 50 % propojeností kvantových bitů. Tyto procesory jsou již schopné redukce chybovosti při výpočtech. Nejlepší procesory dosahují až 5 logických qubitů s nízkou chybovostí a je na nich možné simulovat určité molekuly. Kvantové počítače se již dají využít k určitým úkolům, které by byly pro klasické počítače časově velmi náročné. U kvantových počítačů se jedná převážně o jejich vývoj s občasným praktickým využitím ve výzkumu. Pomalu se začíná implementovat kvantová kryptografie. Běžný člověk si změny ve svém životě zatím nevšimne.

10.2 Předpověď 2030

V roce 2030 jsou kvantové supravodivé procesory na úrovni 2000 kvantových bitů s 60 % procentním propojením mezi qubity. Kvantové počítače na bázi iontových pastí dosahují 1200 qubitů s 80 % propojenost mezi qubity. Fotonové procesory dosahují 2500 qubitů při 70% propojenosti mezi kvantovými bity. Tyto procesory již zvládají korekci chyb na dostatečně dobré úrovni. Objevují se jiné technologie pro kvantové počítače, které by mohly být do budoucna slibnější. Tyto procesory již zvládají korekci chyb na dostatečně dobré úrovni. V praxi se dají využít v mnoha odvětvích. Běžně se budou využívat kvantové počítače pro vývoj léků. Strojové učení pro vývoj materiálů, optimalizaci pracovního prostředí a jiné již v provozu. Kvantové počítače se využívají k optimalizaci veřejné dopravy a společnosti jako je Google optimalizují dopravu díky svým mapám za pomocí kvantových počítačů. Google také začíná využívat kvantové modelování osobnosti svých uživatelů. IBM, Microsoft i Google pracují na kvantové umělé inteligenci. Za pomocí kvantových počítačů se také zefektivnilo cestování do vesmíru. Kvantové počítače lépe vymodelují tvary vesmírných raket a také optimalizují jejich paliva. Začínají se objevovat roboti na domácí pomoc.

10.3 Předpověď 2040

Kvantové počítače již dosahují statisíců qubitů. Sjednotily se typy kvantových procesorů. Kvantové počítače se již staly běžnou součástí našeho života. Tempo našeho života se ještě zrychlilo. Díky kvantovým počítačům dokážeme již od narození vědět, jaké máme genetické předpoklady a určité nedostatky dokážeme napravovat. Lékaři už téměř nemusí analyzovat zranění, zvládne to za ně kvantový počítač. Za pomocí pokroků se nám povedlo zastavit globální změny. Dokážeme perfektně předvídat počasí. Jsme schopni léčit rakovinu. Protézy budou digitálně propojené s mozkem a jen za pomocí myšlenek jimi bude možné pohybovat. Kvantový internet je již v provozu.

Tyto předpovědi, i když mohou v současné době znít jako mimo realitu nebo ze sféry sci-fi, tak jsem přesvědčen, že alespoň část těchto předpovědí se stane skutečností v podobném časovém horizontu. A bude to právě s pomocí kvantových počítačů

11 DOPADY NA SVĚT

Kvantové počítače jako takové budou mít velký dopad na svět, a ještě větší dopad pro lidstvo. Víme, že kvantové počítače pracují na bázi kvantové mechaniky. V současnosti rozumíme jen určité části. Za pomocí zkoumání a vývoje kvantových počítačů budeme schopni nahlédnout na fungování vesmíru jako takového.

Enviromentální dopady na svět by mohly být velmi pozitivní, pokud se nám podaří vyvinou lepší kvantové počítače v poměrně krátké době. Pomohlo by nám to při zkoumání a vylepšování všech procesů, které zatěžují atmosféru Země. Jak bylo řečeno, výroba hnojiv, čistší energie za pomocí fotovoltaiky, materiály ve stavebnictví a mnoho dalšího. Při přesnějším předvídání počasí bychom mohli limitovat ztráty na životech. Byli bychom schopni reagovat dříve v zemědělství a třeba ještě úrodu zachránit.

Dopady na lékařství již v současnosti začínají být znát. D-Wave kvantové annealery napomáhaly během krize covid-19, klinika pracující na lécích má již zarezervovaný supravodivý kvantový počítač od IBM. V současnosti jde jen o krůčky, ale v blízké budoucnosti půjde jistě o kroky a dojde rychlejšímu vývoji léků. Tyto počítače také v budoucnu poslouží k analýze problémů pacienta a k jeho rychle rekonvalescenci.

Dopravní a logistický sektor využije možností strojového učení, ať už při vývoji lepších materiálů, tak při organizaci provozu. Přechod na elektromobilitu není bez problémů, ale díky potenciální optimalizaci spotřeby energie a lepším akumulátorům by to nemuselo být bolestivé. Kvantové počítače by také napomohly při řešení problémů se skladováním produktů na skladě.

Kryptografie bude zajisté patřit k jednomu z polarizačních bodů pro kvantové počítače. Možnost zneužití hrubé výpočetní síly k prolamování hesel. Prolomení peněženek kryptoměn nebo dalšího zneužití. Naštěstí se již v současnosti svět připravuje na kvantovou éru za pomocí nového šifrování. Kvantová komunikace by nám v budoucnosti měla dovolit nejen bezpečnou komunikaci, ale také kvantový internet.

ZÁVĚR

V úvodu práce jsem vám představil kvantové počítače. Vysvětlil jsem, jak pracují, jak reagují na prostředí a jaké výhody s nimi přichází. Zběžně jsem poukázal na důležité body v historii vývoje kvantových počítačů, a poté jsem přešel k vysvětlování různých architektur kvantových bitů. Zvážil jsem jejich výhody i nevýhody. Následovalo využití kvantových počítačů, kde jsem se pokusil přiblížit budoucnost s kvantovými počítači. V praktické části jsem uvedl společnosti, které se podílí na vývoji této nové technologie a u těch největších jsem nevynechal jejich historii. U prognostických metod jsem popsal jejich funkci a způsob použití. Poté jsem analyzoval prostředí skrze země, které se účastní kvantové soutěže. Následovala prognóza vývoje v podobě nárůstu kvantových bitů a dále jsem sepsal ve třech obdobích budoucnost s kvantovými počítači. A na konci jsem popsal, jaké dopady bude mít kvantový počítač na svět.

12 BIBLIOGRAFIE

(1) BERNHARDT, Chris. *Quantum Computing For Everyone*. 2019. Massachusetts Institute of Technology: The MIT Press, 2019. ISBN 9780262039253.

(2) OLIVER, William. *Introduction to Quantum Computing* [online]. In: . 2019 [cit. 2021-8-1]. Dostupné z: https://www.youtube.com/watch?v=ZuHHgoe2B0o

(3) Quantum Computing Expert Explains One Concept in 5 Levels of Difficulty [online]. In: . 2018 [cit. 2021-7-31]. Dostupné z: https://www.youtube.com/watch?v=OWJCfOvochA

(4) WILDE, Mark M. *Quantum Information Theory*. Cambridge University Press, 2013. ISBN 978-1-107-03425-9.

(5) *Quantum Supremacy Using a Programmable Superconducting Processor* [online]. In: . 2019 [cit. 2021-8-1]. Dostupné z: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

(6) PRESS, Gil. *27 Milestones In The History Of Quantum Computing* [online]. In: . [cit. 2021-8-1]. Dostupné z: https://www.forbes.com/sites/gilpress/2021/05/18/27-milestones-in-the-history-of-quantum-computing/

(7) *Volkswagen optimizes traffic flow with quantum computers* [online]. In: . 2019 [cit. 2021-8-1]. Dostupné z: https://www.volkswagenag.com/en/news/2019/10/volkswagen-optimizes-traffic-flow-with-quantum-computers.html#

(8)*Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press, 2018. ISBN 978-0-309-47969-1.

(9) ŠTĚDROŇ, Bohumír, Marcela PALÍŠKOVÁ, Zdeněk SOUČEK, Antonín DVOŘÁK a Pavel TILINGER. *Prognostika*. V Praze: C.H. Beck, 2019. Beckova edice ekonomie. ISBN 978-80-7400-746- 0.

(10) ŠTĚDROŇ, Bohumír. *Prognostické metody a jejich aplikace*. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN ISBN 978- 80-7179-174-4.

(11) ARTL, J., M. ARTLOVÁ a E. RUBLÍKOVÁ. *Analýza ekonomických časových řad s příklady*. Praha, 2002. Skripta. VŠE Praha.

(12) *About IBM* [online]. [cit. 2021-8-11]. Dostupné z: https://www.ibm.com/about

(13) *On "Quantum Supremacy"* [online]. In: PEDNAULT, Edwin, John GUNNELS, Dmitri MASLOV a Jay GAMBETTA. 21.10.2019 [cit. 2021-8-12]. Dostupné z: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

(14) PRESKILL, John. *Quantum computing and the entanglement frontier* [online]. Pasadena, CA, USA, 2012 [cit. 2021-8-12]. Dostupné z: https://arxiv.org/abs/1203.5813. California Institute of Technology.

(15) *Macrotrends* [online]. [cit. 2021-8-12]. Dostupné z: https://www.macrotrends.net/

(16) GAMBETTA, Jay. *IBM's Roadmap For Scaling Quantum Technology* [online]. In: . [cit. 2021-8-12]. Dostupné z: https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

(17) HOSCH, William L. a Mark HALL. *Google* [online]. [cit. 2021-8-12]. Dostupné z: https://www.britannica.com/topic/Google-Inc

(18) *Google* [online]. [cit. 2021-8-15]. Dostupné z: https://www.google.com/

(19) *Honeywell* [online]. [cit. 2021-8-15]. Dostupné z: https://www.honeywell.com

(20) Honeywell Sets Another Record For Quantum Computing Performance [online]. [cit. 2021-8-15]. Dostupné z: https://www.honeywell.com/us/en/news/2021/07/honeywell-sets-another-record-for-quantum-computing-performance

(21) *Honeywell teams with U.K. startup on a trio of quantum computing advances* [online]. [cit. 2021-8-15]. Dostupné z: https://fortune.com/2021/07/21/honeywell-cambridge-quantum-computing-error-correction-quantum-volume-breakthroughs/

(22) *How BMW Can Maximize Its Supply Chain Efficiency with Quantum* [online]. [cit. 2021-8-15]. Dostupné z: https://www.honeywell.com/us/en/news/2021/01/exploring-supply-chain-solutions-with-quantum-computing

(23) *Can Quantum Improve Phone Batteries? Samsung Explores the Possibility* [online]. [cit. 2021-8-15]. Dostupné z: https://www.honeywell.com/us/en/news/2021/02/samsung-explores-quantum-computing-possibilities

(24) *Get to Know Honeywell's Latest Quantum Computer System Model H1* [online]. [cit. 2021-8-15]. Dostupné z: https://www.honeywell.com/us/en/news/2020/10/get-to-know-honeywell-s-latest-quantum-computer-system-model-h1

(25) *Discover the Quantum AI campus* [online]. [cit. 2021-8-16]. Dostupné z: https://quantumai.google/learn/lab

(26) *Our quantum computing journey* [online]. [cit. 2021-8-16]. Dostupné z: https://quantumai.google/learn/map

(27) Day 1 opening keynote by Hartmut Neven (Quantum Summer Symposium 2020). *Youtube.com* [online]. [cit. 2021-8-16]. Dostupné z: https://www.youtube.com/watch?v=TJ6vBNEQReU

(28) BELLIS, Mary. *A Short History of Microsoft* [online]. [cit. 2021-8-16]. Dostupné z: https://www.thoughtco.com/microsoft-history-of-a-computing-giant-1991140

(29) LOVE, Julie. *There's no better time to join the quantum computing revolution* [online]. [cit. 2021-8-16]. Dostupné z: https://cloudblogs.microsoft.com/quantum/2020/10/13/join-quantum-computing-revolution-training-resources/

(30) SIMONITE, Tom. *Microsoft's Big Win in Quantum Computing Was an 'Error' After All* [online]. [cit. 2021-8-16]. Dostupné z: https://www.wired.com/story/microsoft-win-quantum-computing-error/

(31) KOUWENHOVEN, Leo P. a další. *Large zero-bias peaks in InSb-Al hybrid semiconductor- superconductor nanowire devices* [online]. 2018, , 36 [cit. 2021-8-16]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/2101/2101.11456.pdf

(32) KOUWENHOVEN, Leo P. a další. Retraction Note: Quantized Majorana conductance. *Nature* [online]. , 1 [cit. 2021-8-16]. Dostupné z: https://www.nature.com/articles/s41586-021-03373-x

(33) *Xanadu* [online]. [cit. 2021-8-16]. Dostupné z: https://www.xanadu.ai/

(34) VERNON, Zachary. *Scaling Photonic Quantum Computers* [online]. In: . [cit. 2021-8-17]. Dostupné z: https://www.youtube.com/watch?v=vF6PkXmo2XA

(35) *IonQ* [online]. [cit. 2021-8-17]. Dostupné z: https://ionq.com/company

(36) HACKETT, Robert. *Startup IonQ drastically ups the quantum computing ante* [online]. [cit. 2021-8-17]. Dostupné z: https://fortune.com/2020/10/01/ionq-quantum-computer-most-powerful-honeywell-ibm-google/

(37) PROTALINSKI, Emil. *IonQ's roadmap: Quantum machine learning by 2023, broad quantum advantage by 2025* [online]. [cit. 2021-8-17]. Dostupné z: https://venturebeat.com/2020/12/09/ionq-roadmap-quantum-machine-learning-2023-broad-quantum-advantage-2025/

(38) *Atom Computing* [online]. [cit. 2021-8-17]. Dostupné z: https://www.atom-computing.com/

(39) TAKAHASHI, Dean. *Atom Computing raising $15M to create Phoenix quantum computing system* [online]. 21.7.2021 [cit. 2021-8-17]. Dostupné z: https://venturebeat.com/2021/07/21/atom-computing-raising-15m-to-create-phoenix-quantum-computing-system/

(40) SHANKLAND, Stephen. *Intel upgrades quantum computer ambitions with new control chip* [online]. 2020 [cit. 2021-8-17]. Dostupné z: https://www.cnet.com/tech/computing/intel-upgrades-quantum-computer-ambitions-with-new-control-chip/#:~:text=Intel%20unveiled%20on%20Thursday%20its%20Horse%20Ridge%202,future%20quantum%20processors%20with%20thousands%20or%20more%20qubits.

(41) *Amazon Braket* [online]. [cit. 2021-8-17]. Dostupné z: https://aws.amazon.com/braket/

(42) *ColdQuanta Reaches Quantum Computer Milestone By Demonstrating Immense Scalability of 'Cold Atom' Processor Approach* [online]. 7.8.2021 [cit. 2021-8-17]. Dostupné z: https://www.globenewswire.com/news-release/2021/07/07/2259086/0/en/ColdQuanta-Reaches-Quantum-Computer-Milestone-By-Demonstrating-Immense-Scalability-of-Cold-Atom-Processor-Approach.html

(43) TIMMER, John. *Quantum-computing startup Rigetti to offer modular processors* [online]. 29.6.2021 [cit. 2021-8-17]. Dostupné z: https://arstechnica.com/science/2021/06/quantum-computing-startup-rigetti-to-offer-modular-processors/

(44) *PsiQuantum* [online]. [cit. 2021-8-17]. Dostupné z: https://psiquantum.com/

(45) DIVINCENZO, David P. *The Physical Implementation of Quantum Computation* [online]. , 9 [cit. 2021-8-17]. Dostupné z: https://arxiv.org/pdf/quant-ph/0002077.pdf

(46) MANDELBAUM, Ryan F. *What Is Quantum Volume, Anyway?* [online]. [cit. 2021-8-18]. Dostupné z: https://medium.com/qiskit/what-is-quantum-volume-anyway-a4dff801c36f

(47) *Quantum Computing in the NISQ era and beyond* [online]. Pasadena, CA, USA, 2018 [cit. 2021-8-18]. Dostupné z: https://arxiv.org/pdf/1801.00862.pdf. California Institute of Technology.

(48) ADITYA, J. a P. SHANKAR RAO. *Quantum Cryptography* [online]. 2005, , 6 [cit. 2021-8-19]. Dostupné z: https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf

(49) *Quantum Cryptography, Explained* [online]. [cit. 2021-8-19]. Dostupné z: https://quantumxc.com/quantum-cryptography-explained/

(50) *Exploring quantum computing use cases for healthcare* [online]. 2020, , 10 [cit. 2021-8-19]. Dostupné z: https://www.ibm.com/downloads/cas/8QDGKDZJ

(51) What Can Quantum Computing Do To Healthcare? [online]. 2019 [cit. 2021-8-19]. Dostupné z: https://medicalfuturist.com/quantum-computing-in-healthcare/

(52) ŠTĚDROŇ, Bohumír a kolektiv. *Právo a umělá inteligence*. Plzeň: Aleš Čeněk, 2020. ISBN 978-80-7380-803-7.

(53) TensorFlow Quantum [online]. [cit. 2021-8-19]. Dostupné z: https://www.tensorflow.org/quantum

(54) HUANG, Hsin-Yuan, Michael BROUGHTON, Jarrod R. MCCLEAN a Masoud MOHSENI. *Characterizing quantum advantage in machine learning by understanding the*

power of data [online]. [cit. 2021-8-19]. Dostupné z: https://blog.tensorflow.org/2020/11/characterizing-quantum-advantage-in.html

(55) *Forecasting the Weather Using Quantum Computers* [online]. [cit. 2021-8-19]. Dostupné z: https://1qbit.com/blog/quantum-computing/forecasting-the-weather-using-quantum-computers/

(56) Exploring quantum computing use cases for financial services [online]. [cit. 2021-8-19]. Dostupné z: https://www.ibm.com/downloads/cas/2YPRZPB3

(57) MIHULKA, Stanislav. *Čína spustila první kvantovou komunikační síť* [online]. [cit. 2021-8-19]. Dostupné z: https://www.osel.cz/11542-cina-spustila-prvni-kvantovou-komunikacni-sit.html

(58) LETZTER, Rafi. *China's Quantum-Key Network, the Largest Ever, Is Officially Online* [online]. [cit. 2021-8-20]. Dostupné z: https://www.livescience.com/61474-micius-china-quantum-key-intercontinental.html

(59) GOLED, Shraddha. *Top Countries Pumping Money Into Quantum Computing Technology* [online]. [cit. 2021-8-20]. Dostupné z: https://analyticsindiamag.com/top-countries-pumping-money-into-quantum-computing-technology/

(60) PAN, Jian-Wei a další. *Quantum computational advantage using photons* [online]. , 23 [cit. 2021-8-20]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/2012/2012.01625.pdf

(61) *Chinese researchers to send an 'uncrackable' quantum message to space* [online]. [cit. 2021-8-20]. Dostupné z: https://www.livescience.com/super-secure-quantum-messages-headed-to-space.html

(62) PAN, Jian-Wei a další. *Strong quantum computational advantage using a superconducting quantum processor* [online]. In: . s. 22 [cit. 2021-8-20]. Dostupné z: https://arxiv.org/pdf/2106.14734.pdf

(63) *OpenSuperQ* [online]. [cit. 2021-6-10]. Dostupné z: https://opensuperq.eu/

(64) *Finland selects IQM to build its first quantum computer; to deliver a 50-qubit machine by 2024.* [online]. [cit. 2021-8-20]. Dostupné z: https://www.meetiqm.com/articles/press-releases/finland-selects-iqm-to-build-its-first-quantum-computer-to-deliver-a-50-qubit-machine-by-2024/

(65) CHOW, Jerry, Oliver DIAL a Jay GAMBETTA. *IBM Quantum breaks the 100-qubit processor barrier* [online]. 2021 [cit. 2022-01-05]. Dostupné z: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle

(66)*Quantum computing global market projections and forecast comparison 2017 to 2030 (in million U.S. dollars)* [online]. In: . [cit. 2022-01-06]. Dostupné z: https://www.statista.com/statistics/936010/quantum-computing-future-market-outlook-forecast/

(67) *IBM: Quantum Computing* [online]. [cit. 2022-01-06]. Dostupné z: https://www.ibm.com/blogs/research/category/quantcomp/?mhsrc=ibmsearch_a&mhq=quantum

(68) *Size of the enterprise quantum computing market by region from 2017 to 2030 (in million U.S. dollars)* [online]. In: . [cit. 2022-01-06]. Dostupné z: https://www.statista.com/statistics/962870/global-enterprise-quantum-computing-market-by-region/

SEZNAM OBRÁZKŮ

Evidence výpůjček

Prohlášení:

Dávám svolení k půjčování této bakalářské práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

Jméno a příjmení: Jan Kuchař

V Praze dne: 06. 01. 2022 Podpis:

Jméno	**Oddělení/Pracoviště**	**Datum**	**Podpis**