STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**KVANTOVÉ POČÍTAČE A ICH VPLYV NA BEZPEČNOSŤ**

Ročníková práca

**IVAN POLÁK**

2024

Obsah

Obsah 2

Anotácia 3

1 Kvantové počítače 4

1.1 Vznik a vývoj 4

1.2 Základy kvantovej mechaniky a ich aplikácia v kvantových počítačoch 4

1.3 Výhody a výzvy 6

1.4 Budúcnosť 6

1.5 Qubity a kvantové hradlá 6

1.6 Kvantové algoritmy 7

1.7 Aplikácie kvantových počítačov 7

1.8 Bezpečnosť a kvantové počítače 7

1.9 Faktorizácia veľkých čísel 8

1.10 Bezpečnostné protokoly 8

1.10.1 Post-quantum kryptografia 8

1.10.2 Overovanie a šifrovanie 9

1.10.3 Etické aspekty 9

1.10.4 RSA a 256-bitové šifrovanie 9

1.11 Architektúra kvantových počítačov 10

1.12 Perspektívy a výzvy 10

1.13 Príprava na vek kvantových počítačov 10

1.13.1 Výskum a vývoj 10

1.13.2 Vzdelávanie a odborná príprava 10

1.13.3 Vytváranie kvantovo odolných kryptografických systémov 10

1.13.4 Testovanie a overovanie existujúcich systémov 11

1.13.5 Spolupráca a výmena poznatkov 11

1.13.6 Etické a právne otázky 12

2 Vývoj produktu 13

2.1 Výber formátu 13

2.2 Hľadanie zdrojov 13

2.3 Overovanie zdrojov 13

2.4 Porozumenie problematike 13

2.5 Stanovenie učebného cieľa 14

2.6 Stanovanie výkonových štandardov 14

Záver 15

Zoznam použitej literatúry 16

Anotácia

V súčasnosti, informačné technológie dominujú našej spoločnosti a poskytujú nám obrovský potenciál v rôznych oblastiach. Kvantové počítače sú revolučnou technológiou, ktorá by mohla zmeniť paradigmu v oblasti výpočtov a riešenia zložitých problémov. Ich schopnosť manipulovať s kvantovými bitmi - kvantovými stavmi - prináša nové možnosti v oblasti kryptografie, optimalizácie a simulácií. V tejto práci sa zameriam na preskúmanie princípov, výhod a obmedzení kvantových počítačov. Budem analyzovať ich potenciálne využitie v rôznych odvetviach, ako aj súčasné výzvy a obavy týkajúce sa ich rozvoja. Verím, že tento pohľad na kvantové počítače prinesie nové poznatky a perspektívy do diskusií o budúcnosti výpočtovej technológie a jej vplyvu na spoločnosť.

**Annotation**

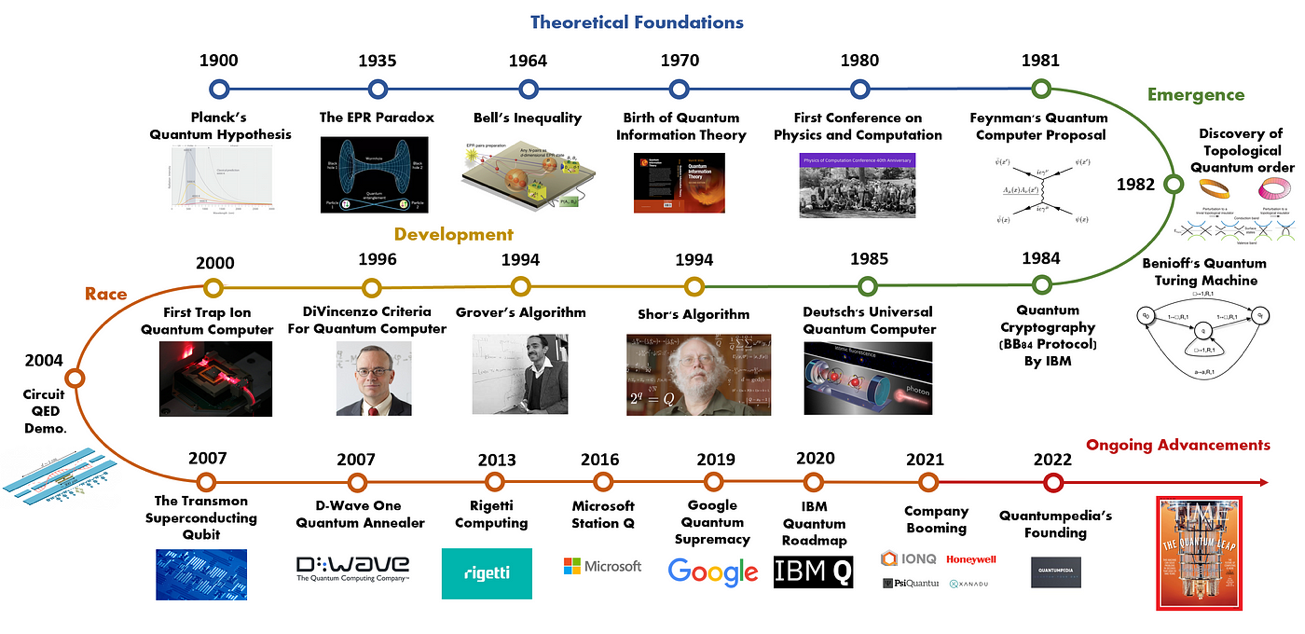
Currently, information technologies dominate our society and provide us with tremendous potential in various areas. Quantum computers are a revolutionary technology that could change the paradigm in computation and solving complex problems. Their ability to manipulate quantum bits - quantum states - brings new possibilities in cryptography, optimization, and simulations. In this paper, I will focus on exploring the principles, advantages, and limitations of quantum computers. I will analyze their potential applications in various industries, as well as current challenges and concerns regarding their development. I believe that this perspective on quantum computers will bring new insights and perspectives to discussions about the future of computing technology and its impact on society.

1. Kvantové počítače

Kvantové počítače predstavujú revolučný pokrok vo svete výpočtovej technológie. Ich schopnosť vykonávať výpočty na úrovni, ktorá je neuskutočniteľná pre klasické počítače, otvára dvere k novým možnostiam v mnohých oblastiach, vrátane vedy, priemyslu a vojenských aplikácií.

* 1. Vznik a vývoj

V roku 1981 Richard Feynman predstavil myšlienku vytvorenia počítačov založených na princípoch kvantovej mechaniky. Avšak prvý skutočný krok smerom k vývoju kvantových počítačov nastal v roku 1994, keď Peter Shor predstavil algoritmus na efektívne faktorizovanie veľkých čísel, čo by mohlo mať významné následky pre kryptografiu. Tieto významné udalosti môžeme vidieť na grafe na obrázku 1. ‎[2]



Obrázok 1 – História ‎[2]

* 1. Základy kvantovej mechaniky a ich aplikácia v kvantových počítačoch

Kvantové počítače, inšpirované princípmi kvantovej mechaniky, predstavujú revolúciu vo svete výpočtovej technológie. Ich jadro tvoria koncepty ako superpozícia, prepletenosť a zrážková pravdepodobnosť, ktoré nám otvárajú dvere k novým výpočtovým možnostiam. Kvantová mechanika je teória, ktorá sa zaoberá správaním veľmi malých častíc na mikroskopickej úrovni. Na rozdiel od klasických počítačov, kvantové počítače využívajú qubity namiesto bitov, ktoré môžu byť v superpozícii rôznych stavov a vzájomne prepletené. Tieto koncepty poskytujú kvantovým počítačom výnimočnú výpočtovú silu. ‎[4]

**Superpozícia - Rôzne možnosti stavu**

Superpozícia umožňuje qubitom existovať v kombinácii rôznych stavov s rôznymi pravdepodobnosťami, čo umožňuje paralelné vykonávanie viacerých operácií súčasne. Na rozdiel od klasických bitov, ktoré môžu byť buď 0 alebo 1, qubity môžu byť v superpozícii týchto stavov, čo poskytuje kvantovým počítačom neuveriteľnú výpočtovú flexibilitu. ‎[11]

**Prepletenosť - Vzájomné prepojenie**

Prepletenosť je jav, ktorý umožňuje kvantovým časticiam byť vzájomne spojené tak, že ich vlastnosti nie je možné nezávisle popísať. Tento fenomén poskytuje kvantovým počítačom neuveriteľnú paralelnú výpočtovú silu a umožňuje im vykonávať komplexné operácie s vysokou efektivitou. ‎[12]

**Zrážková pravdepodobnosť - Pravdepodobnostné vyhodnocovanie**

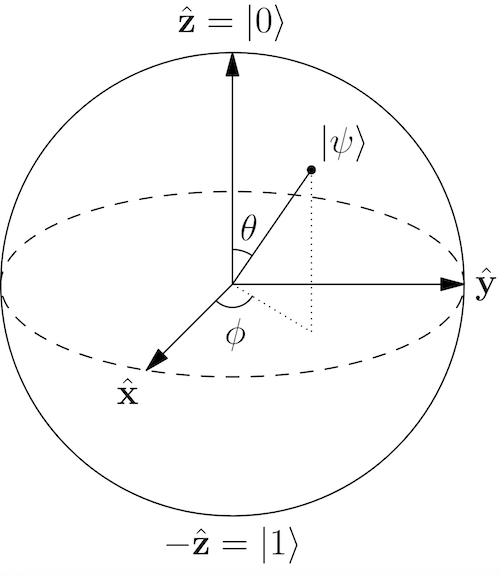
Zrážková pravdepodobnosť je kvantový jav, ktorý popisuje pravdepodobnosť, že kvantové častice sa budú správať ako vlny a prechádzať cez prekážky. Tento jav je základom experimentov, ktoré demonštrujú kvantovú povahu častíc a ich schopnosť vykazovať interferenčné vzory. ‎[12]

**Heisenbergov princíp neurčitosti - Neurčitosť v meraniach**

Heisenbergov princíp neurčitosti hovorí, že nie je možné presne určiť súčasne polohu a hybnosť kvantovej častice. Tento princíp má dôležité dôsledky pre meranie a pozorovanie kvantových systémov, a zároveň ovplyvňuje spôsob, ako sú merané a manipulované kvantové počítače. ‎[11]

**Aplikácia v kvantových počítačoch**

Základy kvantovej mechaniky tvoria kľúčový základ kvantových počítačov a umožňujú im vykonávať neuveriteľné výpočty a úlohy. Porozumenie týchto princípov nám pomáha lepšie chápať, ako kvantové počítače fungujú a ako môžu byť využité na riešenie komplexných problémov v rôznych odvetviach vedy a technológie. ‎[4]



Obrázok 2 - Qubit ‎[3]

* 1. Výhody a výzvy

Hlavnou výhodou kvantových počítačov je ich schopnosť riešiť určité problémy rýchlejšie, ako je možné pomocou klasických počítačov. To otvára dvere k novým možnostiam v oblastiach ako kryptografia, chemické a biologické simulácie, optimalizácia a umelá inteligencia. Avšak vývoj kvantových počítačov je stále v ranom štádiu a existujú mnohé technické výzvy, ktoré je potrebné prekonať, ako sú chyby v kvantovom hardvéri, nedostatok škálovateľnosti a náročné algoritmy. ‎[2]‎[3]‎[4]‎[10]

* 1. Budúcnosť

Budúcnosť kvantových počítačov je plná možností a prísľubov. Ich úplné využitie by mohlo mať významné dôsledky pre mnohé odvetvia a priniesť nové technologické inovácie, ktoré by mohli zmeniť spôsob, akým vykonávame výpočty a riešime komplexné problémy. Toto je len začiatok cesty, ktorá nás zavedie do sveta kvantových počítačov. Čakajú nás vzrušujúce objavy, technologické pokroky a nové aplikácie, ktoré môžu zmeniť náš svet. ‎[2]‎[1]

* 1. Qubity a kvantové hradlá

Qubity sú základné jednotky kvantových počítačov, ktoré môžu byť v superpozícii alebo prepletené. Kvantové hradlá sú kvantové verzie klasických logických hradiel, ktoré umožňujú manipulovať s qubitmi a vykonávať výpočtové operácie ‎[4].

* 1. Kvantové algoritmy

Existuje niekoľko kvantových algoritmov, ktoré umožňujú riešiť určité problémy rýchlejšie, ako je možné pomocou klasických algoritmov. Medzi najznámejšie kvantové algoritmy patria Shorov algoritmus na faktorizáciu veľkých čísel a Groverov algoritmus na vyhľadávanie v nezoradených databázach. ‎[4]

* 1. Aplikácie kvantových počítačov

Kvantové počítače majú potenciál revolučne ovplyvniť rôzne odvetvia, vrátane kryptografie, farmaceutického výskumu, umelého učenia a optimalizácie. Ich výkonnosť by mohla viesť k vytváraniu nových liekov, optimalizácii logistických procesov a vytváraniu nových kryptografických štandardov. ‎[1]‎[4]‎[9]

Tabuľka 1 Aplikácie kvantových počítačov ‎[9]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aplikácia** | **Kvalita predpovede potrebného počtu qubitov** | **Príklad využitia** | **Potrebných qubitov** | **Predpokladaná potrebná maximálna chybovosť brány** |
| Prelomenie kryptografie | Dobrá | Prelomenia RSA-2048 | ~ 20 miliónov | ~ 0.1% |
| Chémia | Stredná | Simulácia FeMoco | ~ 4 milióny | ~ 0.1% |
| Optimalizácia / AI | Zlá | ? | ? | ? |

* 1. Bezpečnosť a kvantové počítače

Kvantové počítače, svojou povahou a schopnosťami, zasahujú do oblasti kryptografie a zabezpečenia informácií. Zatiaľ čo môžu priniesť inovácie v mnohých smeroch, môžu aj ohroziť existujúce kryptografické systémy, ktoré sú založené na problémoch, ktoré sú pre klasické počítače ťažké na vyriešenie. ‎[1]‎[10]

Graf 1 Odhady expertov kedy budú kvantové počítače schopné prelomiť RSA-2048 do 24 hodín ‎[10]

* 1. Faktorizácia veľkých čísel

Jedným z najznámejších algoritmov v oblasti bezpečnosti týkajúcej sa kvantových počítačov je Shorov algoritmus, ktorý má schopnosť faktorizovať veľmi veľké čísla v čase, ktorý je exponenciálne menší ako je tomu v prípade klasických algoritmov. Faktorizácia veľkých čísel je základom mnohých kryptografických protokolov, ako napríklad RSA (Rivest-Shamir-Adleman) a ECC (Elliptic Curve Cryptography). Ak by kvantové počítače dokázali efektívne faktorizovať veľké čísla, tak by mohli ohroziť bezpečnosť týchto systémov. ‎[4]‎[1]

* 1. Bezpečnostné protokoly

V súčasnosti prebieha veľa výskumu v oblasti kvantových bezpečnostných protokolov. Jedným z príkladov je kvantová distribúcia kľúčov (QKD), ktorá využíva kvantové princípy na vytvorenie nevyhnutného kľúča pre kryptografické účely. Tieto protokoly sú navrhnuté tak, aby boli odolné voči útokom založeným na kvantových algoritmoch. ‎[1]‎[4]

* + 1. Post-quantum kryptografia

Vzhľadom na potenciálnu hrozbu, ktorú kvantové počítače predstavujú pre existujúce kryptografické systémy, sa vyvíja koncept post-kvantovej kryptografie. Tieto systémy sú navrhnuté tak, aby boli odolné voči útokom zo strany kvantových počítačov, a teda by mali zostať bezpečné aj v prípade, že by sa takéto počítače stali realitou. ‎[1]‎[4]‎[10]

* + 1. Overovanie a šifrovanie

V oblasti bezpečnosti je kritické, aby sme si boli istí bezpečnosťou overovacích procesov a šifrovaných komunikácií. Kvôli možnému vplyvu kvantových počítačov na tieto procesy je dôležité vyvíjať a implementovať nové technológie a protokoly, ktoré sú odolné voči takýmto hrozbám. ‎[1]‎[4]‎[10]

* + 1. Etické aspekty

Okrem technických otázok je dôležité zvážiť aj etické a spoločenské dôsledky kvantových počítačov v oblasti bezpečnosti. Rýchly rozvoj kvantových technológií si vyžaduje zodpovedný prístup k vývoju a nasadeniu, aby sme zabezpečili, že tieto technológie budú používané v prospech ľudstva a budú slúžiť k zlepšeniu našej bezpečnosti a súkromia. Kvantové počítače prinášajú nové výzvy a príležitosti v oblasti bezpečnosti. Je dôležité monitorovať ich vývoj a prijať opatrenia na zabezpečenie, že naše kryptografické systémy zostanú odolné voči budúcim hrozbám a útokom. ‎[1]‎[4]‎[10]

* + 1. RSA a 256-bitové šifrovanie

Kvantové počítače majú potenciál prelomiť RSA šifrovanie, ktoré sa spolieha na obtiažnosť faktorizácie veľkých čísel. Využitie Shorovho algoritmu umožňuje kvantovým počítačom efektívne faktorizovať čísla. Tento vývoj predstavuje výzvu pre bezpečnosť RSA šifrovania a zdôrazňuje potrebu kvantovo odolných kryptografických algoritmov.

256-bitové šifrovanie je v súčasnosti považované za veľmi bezpečné, pretože exponenciálne zvyšuje počet možných kľúčových kombinácií. Kvantové počítače môžu potenciálne ohroziť túto bezpečnosť pomocou Groverovho algoritmu, ktorý umožňuje vyhľadávanie kľúčov výrazne rýchlejšie než klasické počítače. Napriek tomu by kvantový počítač na prelomenie 256-bitového šifrovania stále potreboval významné množstvo operácií, aj keď by bolo menej než u klasického počítača. ‎[1]‎[4]‎[10]

* 1. Architektúra kvantových počítačov

Existujú rôzne prístupy k vytváraniu kvantových počítačov, vrátane kryogénnych superpočítačov, optických počítačov a iontových pascí. Každá architektúra má svoje výhody a nevýhody a je predmetom aktívneho výskumu. ‎[4]

* 1. Perspektívy a výzvy

Aj keď kvantové počítače majú veľký potenciál, existujú aj výzvy, ktoré je potrebné prekonať, ako sú technické obmedzenia, chyby v kvantovom hardvéri a náročné algoritmy na korekciu chýb. ‎[1]‎[10]

* 1. Príprava na vek kvantových počítačov

Kvantové počítače predstavujú revolučný pokrok vo výpočtovej technológii, ktorý prináša nové možnosti aj nové výzvy. Ako sa svet pripravuje na túto hrozbu a očakáva využiť príležitosti, ktoré kvantové počítače prinášajú? ‎[1]‎[4]‎[10]

* + 1. Výskum a vývoj

S vývojom kvantových počítačov rastie aj záujem o výskum v tejto oblasti. Výskumné inštitúcie a technologické spoločnosti investujú do vývoja nových technológií a algoritmov, ktoré by mohli využiť potenciál kvantových počítačov. Tento výskum zahŕňa nielen hardvér a softvér, ale aj nové matematické a fyzikálne koncepty, ktoré sú potrebné na pochopenie a efektívne využívanie kvantových systémov. ‎[1]‎[4]‎[10]‎[2]

* + 1. Vzdelávanie a odborná príprava

S nástupom kvantových počítačov sa menia aj požiadavky na odborníkov v oblasti informatiky a matematiky. Nové kurzy a študijné programy sa zameriavajú na kvantovú informatiku a kvantovú mechaniku, aby sa pripravili budúci programátori a vedci na prácu s kvantovými technológiami. Spoločnosti tiež investujú do odbornej prípravy svojich zamestnancov, aby boli schopní pracovať s kvantovými počítačmi a využívať ich potenciál. ‎[4]‎[2]

* + 1. Vytváranie kvantovo odolných kryptografických systémov

S nástupom kvantových počítačov sa zvyšuje aj dopyt po kryptografických systémoch, ktoré sú odolné voči útokom zo strany týchto počítačov. Vedci a inžinieri pracujú na vývoji post-kvantových kryptografických algoritmov, ktoré by mohli ochrániť citlivé informácie aj v prítomnosti kvantových počítačov. ‎[10]

**Úspešne kvantovo odolné kryptografické systémy:**

**Ed25519**: Ed25519 je moderný kryptografický algoritmus založený na eliptických krivkách, ktorý ponúka vysokú úroveň bezpečnosti aj v prítomnosti kvantových počítačov. Tento algoritmus je navrhnutý tak, aby bol odolný voči útokom založeným na faktorizácii veľkých čísel a diskrétnemu logaritmu, čím poskytuje bezpečnú možnosť digitálnej podpisovej schémy. Algoritmus sa používa na generovanie kryptografických kľúčov.

**NTRUEncrypt**: NTRUEncrypt je kryptografický algoritmus na šifrovanie a digitálnu podpisovú schému, ktorá využíva matematické koncepty mriežok. Tento algoritmus je známy svojou odolnosťou voči kvantovým útokom, pretože jeho bezpečnosť nie je založená na ťažkosti faktorizácie veľkých čísel alebo diskrétnemu logaritmu.

**Lattice-based cryptosystems**: Kryptografické systémy založené na mriežkach sú ďalšou skupinou algoritmov, ktoré sú považované za odolné voči kvantovým útokom. Tieto systémy využívajú matematické vlastnosti mriežok na šifrovanie a digitálnu podpisovú schému a sú navrhnuté tak, aby odolali útokom založeným na faktorizácii veľkých čísel.

Tieto príklady ukazujú, že existujú kryptografické systémy, ktoré sú navrhnuté tak, aby boli odolné voči kvantovým útokom a môžu poskytnúť bezpečné riešenia pre komunikáciu a uchovávanie citlivých informácií v dobe nástupu kvantových počítačov. ‎[4]

* + 1. Testovanie a overovanie existujúcich systémov

Svet sa snaží zistiť, aké sú skutočné hrozby, ktoré kvantové počítače predstavujú pre existujúce systémy a technológie. Rôzne organizácie a inštitúcie vykonávajú testy a simulácie, aby posúdili, ako by sa tieto systémy mohli správať v prítomnosti kvantových počítačov a aké sú možné scenáre útokov. ‎[1]

* + 1. Spolupráca a výmena poznatkov

Kvantové počítače vyžadujú multidisciplinárny prístup a spoluprácu medzi rôznymi odbormi a odvetviami. Spoločnosti a výskumné inštitúcie investujú do spolupráce a výmeny poznatkov, aby mohli efektívne využívať potenciál kvantových technológií a riešiť ich výzvy. ‎[4]

* + 1. Etické a právne otázky

S nástupom kvantových počítačov sa otvárajú aj otázky týkajúce sa etiky a práva. Ako chrániť osobné údaje a citlivé informácie pred možnými útokmi kvantových počítačov? Ako zabrániť zneužitiu tejto technológie na účely špionáže a kybernetických útokov? Tieto otázky si vyžadujú pozornosť nielen od technologických spoločností a výskumných inštitúcií, ale aj od vlád a medzinárodných organizácií. ‎[4]

1. Vývoj produktu
   1. Výber formátu

Výber formátu nebol úplne jednoduchý, potreboval som vybrať formát, ktorý nebude mať príliš veľký rozsah, ale zároveň bude schopný prezentovať túto komplikovanú tému. Zvolil som preto formát malej knižky - brožúry. Ciel je mať priestor prezentovať komplikované koncepty a doplniť obsah o obrázky a grafy.

* 1. Hľadanie zdrojov

O kvantových počítačoch som už niečo vedel z mojich obľúbených kanálov na platforme YouTube, preto ma aj táto téma zaujala. V zdrojoch videí týchto kanálov som objavil niektoré dobré zdroje ako napríklad quantumcomputingreport.com (‎[1]). Pomohla mi aj účasť na minuloročnej konferencii na univerzite STU - FEI, kde odborníci z IBM prezentovali o ich vývoji a objavoch v oblasti kvantových počítačov. Vypočul som si dátovú vedkyňu Natašu Plulikovú a kvantovú ambasádorku Zoru Hollú. Ďalšie zdroje som našiel vyhľadávaním na internete priamo počas tvorby práce, takto som našiel napríklad zdroj ‎[5], knihu, ktorú som následne zakúpil ako elektronickú knihu na internete.

* 1. Overovanie zdrojov

Každý jeden zdroj som si overoval, hľadal som citácie tohto zdroja a overoval jeho dôveryhodnosť. Bolo nevyhnutné zabezpečiť, aby informácie použité v produktoch boli spoľahlivé a overené. Preto som venoval dostatočnú pozornosť overovaniu autenticity a dôveryhodnosti každého zdroja, či už ide o odborné štúdie, publikácie od renomovaných expertov alebo online zdroje. Tento proces zahŕňal aj analýzu zdrojových materiálov, ich recenzií a prípadne porovnávanie s ďalšími zdrojmi, aby som sa ubezpečil o ich relevancii a spoľahlivosti. Dôkladné overovanie zdrojov zaručovalo kvalitu a dôveryhodnosť celého produktu.

* 1. Porozumenie problematike

Aj keď som mal už predtým všeobecné znalosti o tejto téme z internetu, nedokázal som úplne porozumieť komplexným problémom a konceptom. Preto som sa musel intenzívne venovať štúdiu tejto témy pred začatím a počas tvorby tejto práce. Tento proces mi pomohol lepšie pochopiť zložité koncepty a problémy, aby som ich mohol následne adekvátne prezentovať v tejto práci a výslednom produkte.

* 1. Stanovenie učebného cieľa

Stanovenie učebného cieľa bolo nevyhnutné pre správne smerovanie vývoja produktu. Cieľom bolo vytvoriť komplexný, ale zároveň zrozumiteľný materiál, ktorý by osvetlil tému kvantových počítačov pre širokú verejnosť. Tento materiál mal poskytnúť základné informácie o fungovaní kvantových počítačov, ich význam v súčasnosti a potenciálne využitie v budúcnosti. Zároveň mal byť ucelený a systematický, aby čitateľ mohol postupne preniknúť do problematiky bez predchádzajúcich znalostí.

* 1. Stanovanie výkonových štandardov

Pri stanovovaní výkonových štandardov som sa zameral na dve hlavné oblasti: obsah a prezentáciu. Obsahovo som sa snažil zabezpečiť, aby produkt pokryl všetky dôležité aspekty kvantových počítačov a bol informatívny, no zároveň prístupný pre laikov. Zároveň som kládol dôraz na jasnosť a prehľadnosť prezentácie, aby čitateľ ľahko pochopil obsah a nebol znechutený prílišnou komplexnosťou. Pre dosiahnutie týchto cieľov som stanovil jasné kritériá hodnotenia a monitoroval ich dodržiavanie počas celého procesu vývoja.

Záver

Pohľad do budúcnosti je fascinujúci, no zároveň aj plný výziev a otázok, ktoré nám prináša éra kvantových počítačov. S ich príchodom sa otvárajú dvere do novej dimenzie technológie, ktorá môže transformovať náš svet a spôsob, akým chápeme výpočtovú silu.

Kvantové počítače nás nútia premýšľať o budúcnosti s nádejou, no zároveň aj s určitou mierou opatrnosti. Ich možnosti sú nepochybne ohromujúce - sľubujú rýchlejšie výpočty, zlepšené metódy kryptografie a nové inovácie, ktoré môžu zmeniť naše životy. Môžu nám pomôcť objavovať nové lieky, optimalizovať procesy výroby a riešiť zložité problémy, ktoré dnes predstavujú neprístupnú prekážku.

Avšak s týmito novými možnosťami prichádzajú aj nové výzvy a riziká. Kvantové počítače by mohli ohroziť bezpečnosť dnešných kryptografických systémov, a tak nás nútia hľadať nové spôsoby ochrany našich údajov. Okrem toho si vyžadujú značné úsilie a investície do výskumu a vývoja, aby sme ich mohli účinne využiť a integrovať do našej spoločnosti. Preto je naliehavé, aby sme sa už teraz začali pripravovať na príchod kvantových počítačov. Potrebujeme investovať nielen do technologických inovácií, ale aj do vzdelávania a osvety, aby sme zabezpečili, že budeme pripravení na výzvy, ktoré nám táto nová éra prinesie. Musíme budovať odolné kryptografické systémy, rozvíjať nové algoritmy a aplikácie a zároveň sledovať etické a sociálne dôsledky týchto technologických zmien.

Sme na prahu doby, ktorá nám prinesie nové príležitosti, ale aj nové záväzky. Ako spoločnosť máme moc ovplyvniť, akým spôsobom sa tieto nové technológie budú používať. S primeraným úsilím, inováciou a spoluprácou môžeme zabezpečiť, že éra kvantových počítačov bude pre nás všetkých prínosom, ktorý povedie k ďalšiemu kroku v našej technologickej a ľudskej evolúcii.

Zoznam použitej literatúry

1. Quantum Computing Report. [online] [cit. 2024-04-12] Dostupné na: [https://quantumcomputingreport.com](https://quantumcomputingreport.com/)
2. A Brief History of Quantum Computing. [online] [cit. 2024-04-12] Dostupné na: <https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0>
3. The promise of quantum money. [online] [cit. 2024-04-17] Dostupné na:  
   <https://www.hpcwire.com/2014/01/07/promise-quantum-money/>
4. PATHEON SPACE ACADEMY - Quantum Computing Explained for Beginners: The Science, Technology, and Impact, ISBN-13 979-8892387200
5. "IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation". [online] [cit. 2016-05-04] Pôvodne dostupné na: <https://www-03.ibm.com/press/us/en/pressrelease/49661.wss> Dostupné na <https://web.archive.org/web/20160505160937/https://www-03.ibm.com/press/us/en/pressrelease/49661.wss>
6. "IBM Quantum Experience Update". [online] [cit. 2017-04-06] Pôvodne dostupné na: <https://quantumexperience.ng.bluemix.net/qstage/#/community/question?questionId=c7a17f4183104ea22ff8e3e8a95f794c> Dostupné na: <https://web.archive.org/web/20190129182024/https://quantumexperience.ng.bluemix.net/qstage/#/community/question?questionId=c7a17f4183104ea22ff8e3e8a95f794c>
7. "Quantum computing gets an API and SDK". [online] [cit. 2017-03-06] Dostupné na: <https://developer.ibm.com/dwblog/2017/quantum-computing-api-sdk-david-lubensky/>
8. "What Is Quantum Computing?". [online] [cit. 2024-04-24] Dostupné na: <https://blogs.nvidia.com/blog/what-is-quantum-computing>
9. "The professional’s guide to Quantum Technology". [online] [cit. 2024-04-24] Dostupné na: <https://www.quantum.amsterdam/part-5-when-can-we-expect-a-useful-quantum-computer-a-closer-look-at-timelines>
10. Dr. MICHELE MOSCA - "A quantum threat timeline report 2023". [online] [cit. 2024-04-24] Dostupné na: <https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2023.pdf>
11. NOUREDINE ZETTILI – Quantum Mechanics: Concepts and Applications, ISBN-10 0470026790, ISBN-13 978-0470026793
12. ZBIGNIEW FICEK - Quantum Physics for Beginners, ISBN-10 9814669385, ISBN-13 978-9814669382