Anitec-Assinform

White Paper

Il Quantum Computing a supporto della trasformazione digitale italiana

a cura del
Comitato Ricerca, Sviluppo e Innovazione
con la collaborazione del CNR

Maggio 2023

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967

Anitec-Assinform

Contributi di:

EUSTEMA S.p.A., IBM S.p.A., INSIEL S.p.A., ITALTEL S.p.A., KEYLON S.r.L., LEONARDO S.p.A., LUTECH S.p.A., LUTECH ADVANCED SOLUTIONS S.p.A., TIM S.p.A.

Anitec-Assinform

Sommario

Executive Summary 5
1. Premessa 7
2. Quadro di riferimento 8
3. Potenzialità della computazione quantistica 12
   3.1. Introduzione al quantum computing 12
   3.2. Le sfide per l'informatica quantistica 14
   3.3. Stato attuale dello sviluppo tecnologico 16
   3.4. Introduzione alla sicurezza resistente agli attacchi quantistici 18
   3.5. Introduzione alla sicurezza delle comunicazioni quantistiche 19
4. Ambiti di applicazione del quantum computing 22
5. Quale strategia adottare 27
6. Use cases e Best practices 29
   6.1. Quantum NLP 29
   6.2. Variational Algorithms 30
   6.3. Il Deep Reinforcement Learning 31
7. Lo sviluppo delle competenze e le proposte di policy per l'adozione della computazione quantistica in Italia 32
8. Conclusioni 37

EXECUTIVE SUMMARY

Il white paper "Il Quantum Computing a supporto della trasformazione digitale italiana" analizza lo scenario dell'*ecosistema quantum* in Italia mettendo in evidenza, l'evoluzione tecnologica in questo settore, le opportunità e le aree di miglioramento e formulando alcune proposte e suggerimenti di policy da mettere in atto.

Nel 2016 i primi processori quantistici sono stati resi disponibili in cloud e da quella data ogni anno raddoppiano la loro potenza. Nel 2021 sono stati costruiti dei processori che sono in grado di riprodurre un numero di stati impossibile per i computer tradizionali. L'azienda canadese Xanadu ha annunciato la release in cloud del suo processore quantistico basato su tecnologia fotonica a 216 qubits. IBM nel 2020 ha presentato una roadmap di rilascio di processori sempre più potenti e nel 2023 si prevede il rilascio del processore quantistico IBM Quantum Condor a 1121 qubit.

Le applicazioni in ambito quantum sono potenzialmente infinite e impattano sui principali settori dell'economia: il mondo dei servizi finanziari, il settore farmaceutico, le comunicazioni sono infatti soltanto alcuni tra i comparti che stanno già investendo avendone colto per tempo le potenzialità.

Le prime iniziative nazionali e i consorzi mettono a fattor comune le risorse disponibili; best practice quali, ad esempio, Il Centro Nazionale HPC e il consorzio guidato dall'INFN e Cineca sono tutte caratterizzate da una stretta collaborazione tra Mondo accademico, Industria e PA.

Il rapido avanzamento delle tecnologie di Quantum computing degli ultimi anni sta generando enormi prospettive circa la possibilità di avere a disposizione sistemi di calcolo capaci di potenze di elaborazione inimmaginabili da raggiungere con i supercalcolatori basati su approcci tradizionali. In tale ottica, è fondamentale pianificare azioni di formazione mirate sia a sviluppare nuove competenze per coloro che già lavorano nell'ambito delle tecnologie dell'informazione, sia alla creazione di nuovi profili professionali espressamente orientati alla programmazione quantistica.

In particolare, all'alba di questa nuova fase tecnologica, sta nascendo dal mondo industriale una richiesta di nuovi profili quali *Il Quantum Scientist*, che ha profonde capacità scientifiche ed è un esperto di teoria e tecnologia quantistica, *Il Quantum Engineer*, che ha una profonda e dettagliata comprensione della tecnologia quantistica e *Il Quantum Developer*, che è

l'equivalente di un programmatore di sistemi o di uno sviluppatore di applicazioni.

Essenziali, in questo processo di formazione delle competenze, risultano essere strette interazioni cicliche tra quattro componenti: ricerca e sviluppo, formazione professionale, settori industriali, servizi e infrastrutture quantistiche.

1. Premessa

Lo sviluppo di un'industria quantistica nazionale sostenibile presuppone l'esistenza di un ecosistema quantistico ben definito e operativo che si ispiri a principi: competenza e cooperazione tra le parti, in particolare tra pubblico e privato.

Il quantum computing e le quantum secure communications costituiscono certamente due tra le aree di maggior potenziale per lo sviluppo di attività di ricerca e sviluppo e delle competenze correlate.

È da notare, inoltre, che, a differenza delle criticità affrontate oltre venti anni fa in preparazione dell'anno 2000 (*millenium bug)*, l'impatto della corrispondente transizione al quantum – indicata come "Y2Q" – è oggi ben noto: rimangono soltanto da definirne le tempistiche e investire in tale direzione.

Anitec-Assinform – l'Associazione che rappresenta le aziende del settore ICT e dell'innovazione digitale – vuole offrire una fotografia dello stato dell'arte delle attività, dei progetti in questo settore e dello stato delle competenze nonché un'indicazione delle azioni necessarie nel prossimo futuro per garantire la piena competitività del Paese in questo campo.

Il Comitato Ricerca, Sviluppo e Innovazione, in collaborazione con il CNR, ha sviluppato due studi: "Il Quantum Computing a supporto della trasformazione digitale italiana" e "Tecnologie Quantistiche per sicurezza delle Comunicazioni Digitali".

Partendo da uno scenario comune, i due white paper affrontano distintamente: le peculiarità e le diverse applicazioni rese disponibili dalla tecnologia quantum applicata all'IT e le prospettive future della sicurezza nelle comunicazioni digitali.

2. QUADRO DI RIFERIMENTO

Dagli albori dell'informatica, la capacità di calcolo è cresciuta esponenzialmente, ma ci sono ancora problemi che i computer di oggi non saranno mai in grado di risolvere. Per esempio, se si pensa a due grandi sfide della società contemporanea, quali la protezione del nostro ecosistema e la lotta alle malattie gravi e incurabili, si vorrebbe che la tecnologia fosse in grado di simulare la struttura chimica di nuovi farmaci e sviluppare materiali in grado di catturare il carbonio e ridurre l'inquinamento su scala globale.

Questi sono alcuni esempi dei problemi attualmente irrisolvibili che vengono esplorati dall'informatica quantistica: si parla di una tecnologia informatica fondamentalmente diversa, da quelle più note e tradizionali che sfrutta le proprietà e i principi della meccanica quantistica per elaborare le informazioni.

Per affrontare queste e altre sfide, si deve aumentare le capacità di calcolo di questo nuovo tipo di computer.

L'informatica quantistica comincia a essere sempre più concreta e alla nostra portata: le imprese cominciano infatti a vedere il valore commerciale di questo nuovo tipo di calcolo. I progressi senza precedenti dello scorso biennio nell'hardware, nello sviluppo del software e nei servizi avallano la forza di questa tecnologia, creando un ecosistema che apre la strada a ulteriori scoperte e aiuta il mercato a prepararne l'adozione.

Nei prossimi anni, i modelli chimici e l'ingegneria dei materiali, l'intelligenza artificiale, i modelli di rischio delle aziende, i calcoli finanziari e le simulazioni numeriche di ingegneria potrebbero tutti trarre beneficio dall'informatica quantistica rendendo possibili operazioni che per ragioni di capacità di memoria o di tempo di esecuzione non possono essere condotte da macchine classiche, consentendo di raggiungere accuratezza nei risultati al di fuori della portata attuale. Molte altre applicazioni sono state identificate da organizzazioni pubbliche e private, centri di ricerca e università di tutto il mondo.

Il valore della computazione quantistica non sarà visibile soltanto a livello commerciale, ma avrà anche importanti impatti sociali e di sostenibilità. I computer quantistici potranno essere usati per migliorare i modelli di previsione in meteorologia, rendere più efficienti i processi produttivi riducendo gli sprechi, aiutare a identificare nuovi materiali e nuove reazioni chimiche che riducano l'impatto ambientale.

È già noto che i computer quantistici del futuro metteranno in crisi alcuni algoritmi crittografici oggi utilizzati per proteggere i nostri dati, ma la comunità scientifica ha già identificato dei nuovi algoritmi resistenti anche ai computer quantistici che sono stati recentemente certificati[1]. Avendo l'attenzione di sostituire per tempo gli algoritmi crittografici vulnerabili, il quantum computing sarà tutt'altro che una minaccia per la sicurezza, bensì potrà essere utilizzato per migliorare le capacità di analisi degli algoritmi che oggi ci permettono di identificare frodi e attacchi informatici e potenziare ulteriormente i benefici introdotti dall'Intelligenza Artificiale.

La comunità scientifica ritiene che gli algoritmi ibridi integrati sulle tecnologie quantistiche denominate *Noisy Intermediate-Scale Quantum* (NISQ) permetteranno di avere applicazioni di interesse commerciale, legate alla simulazione, ai big data e a intelligenza artificiale e machine learning, con un forte impatto sociale, in diversi campi:

- Fintech: miglioramento dei processi decisionali per l'analisi del rischio, l'ottimizzazione del portafoglio investimenti e il contrasto alle frodi.
- Energy: predizione di consumi, produzione da fonti rinnovabili, distribuzione dell'energia su smart grid.
- Farmaceutica-Medicina-Scienza dei materiali: simulazione e test di molecole complesse, interazioni fra farmaci e target per ridurre il costo di nuovi farmaci e vaccini.
- Trasporti: ottimizzazione della logistica.
- Manifatturiero: ottimizzazione processi produttivi e logistica.
- Fluidodinamica complessa: studi sui cambiamenti climatici e inquinamento.
- Cybersecurity: crittografia sicura, fattorizzazione quantistica, comunicazioni sicure.
- Blockchain: sicurezza algoritmi, cifratura.

A oggi le aree del quantum computing relative al Machine Learning e alle problematiche di ottimizzazione sono fra le più promettenti[2].

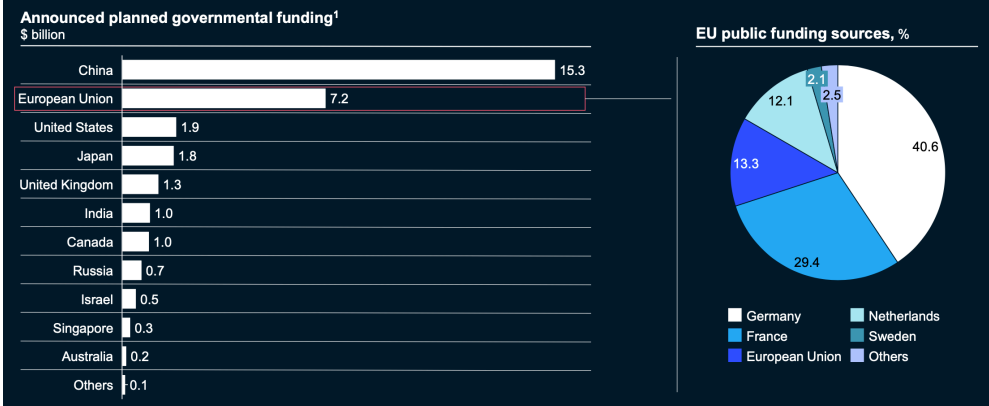
---

[1] Dal NIST, National Institute of Standards and Technology

[2] Boston Consulting Group stima che l'informatica quantistica possa creare un mercato di valore superiore ai 500 miliardi di dollari a maturità tecnologica.

China and the European Union have announced the most public funding planned for QC efforts; Germany has announced most in EU.

Not exhaustive



1. Total historic announced funding; timelines for investment of funding vary per country.

Source: Johnny Kung and Muriam Fancy, *A quantum revolution: Report on global policies for quantum technology*, CIFAR, April 2021; press search June 2021 McKinsey & Company 16

The United States and Canada are still the most active countries in QC, as measured by number of players involved.

Number of QC players, by country

Not exhaustive

+ indicates change in 2H2021

		Start-ups	Incumbent companies	Public/ government organizations	Academic groups
Top 7	United States	60 +1	9	18	64 +1
	Canada	27 +4	0	2	9
	United Kingdom	19	1	2	14 +1
	Japan	13 +1	1	0	7
	France	8	1	3	9
	Germany	8 +1	2	1	7
	China[1]	8 +1	2	12	11
Rest of world		69 +8	1	19	55 +5
Total		**212 +16**	**17**	**57**	**176**

1. There is limited transparency on commercial activity in China and to a lesser extent for Japan. We think Chinese activity in QTs is primarily through government-funded research institutions.

Source: Press and web research; McKinsey analysis McKinsey & Company 20

Fig. 1 Fundings plannings[3]

[3] *Source: Mc Kinsey* – Quantum Technology Monitore – June 2022

Il grafico successivo (Fig. 2) mostra le aree in cui il calcolo quantistico può dare un vantaggio computazionale. I valori di mercato sono stimati come massimo e minimo per ciascuna categoria.

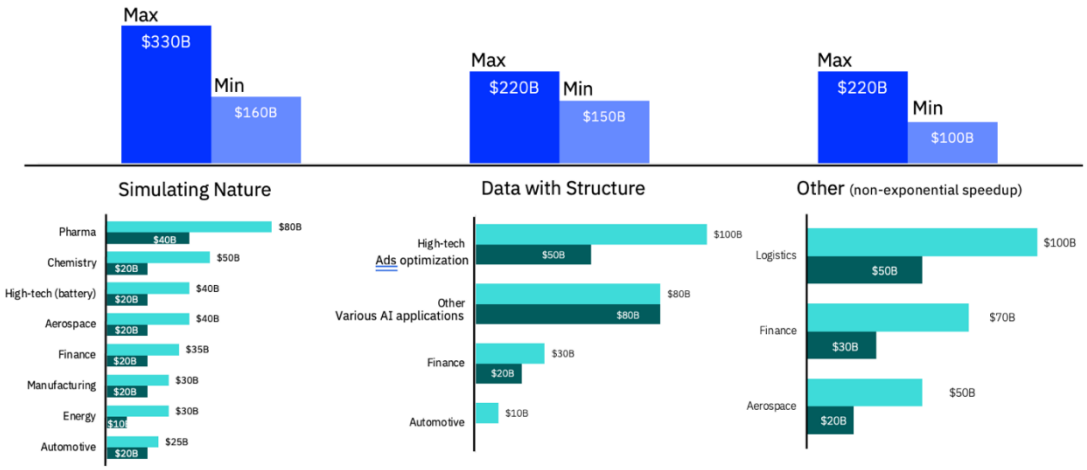


Fig.2 Aree di applicazione Vs Vantaggi computazionali[4]

[4] Source: Boston Consulting Group

3. Potenzialità della computazione quantistica

3.1. Introduzione al quantum computing

Già il premio Nobel per la fisica Richard Feynman negli anni 80 aveva intuito che, per simulare i fenomeni naturali che si basano sui principi della meccanica quantistica, ci sarebbe stato bisogno di un tipo diverso di calcolatori rispetto a quelli che usavamo e che tutt'oggi usiamo.

Questi calcoli devono tener conto delle interazioni che gli elementi interni alle molecole hanno tra loro; al crescere della complessità della molecola queste interazioni crescono in modo esponenziale fino a diventare ingestibili per un calcolatore tradizionale.

Non sono soltanto i calcoli della meccanica quantistica a mettere in crisi i computer per come li conosciamo oggi; anche alcuni problemi di ottimizzazione che possono sembrare banali diventano rapidamente troppo complessi per essere risolti all'aumentare del numero di parametri. Uno degli esempi più noti è "il problema del commesso viaggiatore" nel quale bisogna calcolare il percorso più breve tra un numero noto di città di cui conosciamo le distanze reciproche: il numero di possibili percorsi da considerare cresce in maniera più rapida dell'esponenziale quando aumentiamo il numero di città da visitare prima di tornare a casa; per collegare solo venti città i possibili percorsi da considerare sono miliardi di miliardi.

Nell'ordine delle centinaia di miliardi sono anche i numeri dei parametri adottati dalle reti neurali più recenti e promettenti, eseguite nei modelli di Intelligenza Artificiale attraverso cui i robot sono oggi in grado di interpretare il linguaggio umano (multilingua) e rispondere alle nostre richieste (Q&A).

Esistono infine problemi puramente algebrici che hanno difficoltà analoghe; uno tra questi è la fattorizzazione, ovvero trovare i numeri primi che moltiplicati tra loro danno il numero di partenza; un esercizio che facevamo alle scuole elementari. I nostri computer sono bravissimi a moltiplicare tra loro numeri anche enormi, ma possono aver bisogno di millenni per fare l'operazione inversa appena il numero di cifre comincia a crescere. In pratica per un computer è molto facile risolvere 3 X 5 = 15, ma molto difficile effettuare l'operazione inversa: 15 = 3 X 5. [*Questa potrebbe sembrare solo una curiosità matematica, se non fosse che la maggior parte degli algoritmi crittografici con cui sono*

protetti i nostri dati personali usano meccanismi di questo tipo per impedire l'accesso a chi non è autorizzato].

La domanda che da decenni si pongono i ricercatori è se possa esistere una nuova generazione di computer che possa essere più efficiente nella risoluzione dei problemi sopra enunciata. Una delle possibili risposte sono i computer quantistici. Il succitato problema della fattorizzazione è l'esempio paradigmatico di problemi per i quali l'accelerazione nei tempi di esecuzione che può essere fornita dall'hardware e dal paradigma di calcolo quantistico è non replicabile dall'informatica classica.

I computer in uso quotidianamente effettuano calcoli usando sequenze di 0 e 1. È come se al loro interno ci fossero degli *esserini,* i bit, che possono dire solo Sì o No. Combinando lunghe serie di Sì e No questi *esserini* pronunciano lunghi discorsi che sono i programmi e le applicazioni che usiamo tutti giorni. L'unità di calcolo dei computer quantistici sono invece i qubit che possono essere messi in uno stato di sovrapposizione, una sorta di "forse digitale" che permette al qubit di rimanere indeciso tra il Sì e il No fin quando non vado a leggerlo. Poichè esistono infiniti gradi di indecisione (50% sì e 50% no, 30% sì e 70% no e così via), la sovrapposizione dei qubit fornisce maggiore espressività e permette di gestire informazioni più ricche di quelle dei bit tradizionali.

I qubit possono essere inoltre messi tra loro in *entanglement*: cioè una stretta correlazione tra i loro comportamenti, indipendente dalla distanza.

Queste due proprietà della meccanica quantistica che usano i qubit (sovrapposizione ed *entanglement)* permetteranno di codificare in essi programmi con gradi di complessità molto elevati. Aggiungere un qubit al processore quantistico vuol dire, infatti, poter aggiungere correlazioni dirette con tutti gli altri qubit già presenti; un po' come nel problema del commesso viaggiatore aggiungere una città voleva dire aggiungere nuovi collegamenti con tutte le altre, o come nella simulazione di una molecola aggiungere un elettrone aumentava il numero di interazioni con gli elementi già presenti. Il modo con cui i qubit lavorano insieme nel nuovo modello di computer ci fa capire come questo possa essere affine ai problemi non risolvibili da computer attuali di cui abbiamo appena parlato.

I meccanismi di base della computazione quantistica sono noti da decenni e sono noti anche alcuni algoritmi per potrebbero avvalersi di questo tipo di calcolo sulle diverse piattaforme hardware (attualmente disponibili solo con risorse computazionali più o meno limitate a seconda della tecnologia

impiegata per realizzarle). La fattorizzazione in numeri primi, enunciata poco fa e così difficile da calcolare su un computer attuale, potrebbe essere rapidamente effettuata da un processore quantistico utilizzando l'algoritmo di Shor[5], pubblicato nel 1994.

È necessario quindi preoccuparci per i numeri delle carte di credito che vengono criptate dai siti con chiavi che usano la fattorizzazione? La risposta è negativa; il motivo è che, al momento in cui è scritto questo testo, la carta di credito eventualmente criptata scadrà prima di quando l'umanità sarà in grado di produrre un computer quantistico abbastanza potente da far girare l'algoritmo di Shor.

3.2. Le sfide per l'informatica quantistica

La prima difficoltà che sta alla base della costruzione dei processori quantistici è la realizzazione dei qubit. I qubit sono oggetti molto instabili e vengono disturbati dall'interazione con qualsiasi particella o interferenza possa venire a contatto con essi. Per garantire il loro funzionamento per la durata dell'operazione da effettuare devono essere portate a temperature prossime allo zero assoluto.

Il secondo ambito di studi su qui stanno lavorando i ricercatori sono i linguaggi di programmazione. Le operazioni di base che si possono effettuare sui qubit sono diverse da quelle che siamo abituati ad usare sui bit dei nostri computer.

Questo richiede innanzitutto appositi linguaggi di programmazione di alto e di basso livello (è da notare infatti che esistono almeno due diversi paradigmi di calcolo quantistico universali che sono adeguati a differenti piattaforme hardware). Lo sviluppo di questi linguaggi viene portato avanti dalle stesse aziende che investono nelle piattaforme, si pensi alla libreria Python Qiskit di IBM, a Q# di Microsoft, alle librerie Python Strawberry Fields e Penny Lane sviluppate da Xanadu o a Paddle Quantum sviluppata dal colosso cinese Baidu.

Siamo all'alba di una nuova branca dell'informatica che va scritta partendo dal linguaggio macchina; una splendida opportunità per gli sviluppatori che vorranno partecipare a questa rivoluzione.

[5] L'algoritmo di fattorizzazione di Shor è un algoritmo ideato da Peter Shor nel 1994 per risolvere il problema della fattorizzazione dei numeri interi in numeri primi.

L'ultima sfida riguarda le aziende e i ricercatori che vorranno usare questi processori per le loro applicazioni di business e le loro attività scientifiche. I programmi che oggi usano sui loro calcolatori andranno completamente ripensati per poter sfruttare le potenzialità della computazione quantistica. Alcuni algoritmi già esistono, come quello di Shor, molti altri devono ancora essere scritti.

Il punto debole delle tecnologie di Quantum Computation è inerente alle caratteristiche proprie del mondo quantistico, molto fragile, che genera errori nei calcoli se non viene controllato e mantenuto isolato. Per ottenere un computer quantistico universale, questa fragilità deve essere corretta tramite opportuni codici correttori quantistici: è un settore di ricerca molto promettente, ma siamo ancora lontani dal raggiungimento dell'obiettivo.

La soluzione che sta emergendo e che è alla portata della tecnologia attuale è quella degli algoritmi ibridi, sui quali stanno puntando i principali centri di calcolo europei. Con questo approccio la parte più impegnativa dei calcoli avviene sulla Quantum Processing Unit (QPU) del computer NISQ e la parte più tradizionale su computer classici o supercomputer.

Vale inoltre la pena aggiungere che, al di là della situazione tecnologica corrente (ovvero la NISQ), la visione prevalente sui calcolatori quantistici e il loro impiego è che essi saranno impiegati specificamente per aggredire quelle problematiche intrattabili classicamente e/o quelle routine dove mostrano un concreto vantaggio, e non andranno quindi in completa sostituzione dei processori classici. Ovvero, il paradigma di utilizzo che si prevede per il prossimo decennio (il riferimento del precedente paragrafo alla QPU a fianco di processori tradizionali come CPU e GPU) è al momento ritenuto valido anche sul lungo periodo.

Come osservato sinora, la computazione quantistica ha una lunga storia di ricerca e la sua reale scalabilità sembra ancora molto lontana e figlia di sfide da intraprendere. Perché allora ha senso parlare oggi di questo tipo di computazione? Il motivo è che sono ormai vari anni che i primi processori quantistici sono a disposizione di tutti, attraverso soluzioni cloud.

I maggiori aspetti che dovrebbero essere affrontati sono la formazione di personale qualificato che possa comprendere e utilizzare al meglio una tecnologia altamente complessa quale il quantum, per permetterne lo sviluppo operativo delle soluzioni software.

3.3. Stato attuale dello sviluppo tecnologico

Lo sviluppo dei computer quantistici ha seguito e continua a seguire percorsi e velocità di crescita diversi a seconda della specifica tecnologia (anche detta piattaforma hardware) scelta per implementare i qubit che sono stati descritti nei paragrafi precedenti.

La figura 3 mostra chiaramente la varietà di piattaforme hardware e di attori accademici o industriali coinvolti nel loro sviluppo.

Fig.3 Piattaforme HW e Stakeholder coinvolti[6]

Tra tali piattaforme hardware esistono rilevanti differenze per un ampio spettro di caratteristiche: numero di qubit attualmente implementabili, requisiti dimensionali (SWaP) della macchina, stabilità e tempi di coerenza raggiungibili, requisiti ambientali (ad es. funzionamento criogenico o a temperatura ambiente).

[6] Source: https://thequantuminsider.com/

L'intersezione di tali caratteristiche mostra, a una approfondita analisi, una serie di *trade off* in quanto ciascuna piattaforma possiede al contempo specifiche caratteristiche vantaggiose e altre meno.

Tale *trade off* può essere limitato, se non proprio superato, dall'uso di simulatori avanzati. Essendo tali simulatori agnostici rispetto alle soluzioni fisiche, essi riescono a emulare ogni tecnologia quantistica esistente, permettendo analisi sulle diverse tecnologie pur sfruttando un'unica risorsa.

Lo svantaggio di tali simulatori è la limitata potenzialità (come una disponibilità minore di qubit) che però è superato dalla immediata disponibilità e accessibilità agli stessi.

Nel 2016 i primi processori quantistici sono stati resi disponibili in cloud e da quella data ogni anno raddoppiano la loro potenza. Nel 2021 sono stati costruiti dei processori che sono in grado di riprodurre un numero di stati impossibile per i computer tradizionali. I grandi leader di questa tecnologia a livello internazionale hanno già presentato le loro aspettative sulla crescita della potenza computazionale quantistica nei prossimi anni. L'azienda canadese Xanadu ha annunciato[7] ai primi di Giugno la release in cloud del suo processore quantistico basato su tecnologia fotonica a 216 qubits. IBM nel 2020 ha presentato una roadmap di rilascio di processori sempre più potenti alla quale si sta attenendo strettamente e che già nel 2023 dovrebbero portare al rilascio del processore quantistico IBM Quantum Condor a 1121 qubit (recente è la notizia[8] del rilascio di IBM Quantum Osprey, processore a 433 qubit) potrebbero già essere in grado di portare vantaggi concreti in vari ambiti produttivi e di ricerca.

Nel frattempo, tutte le più grandi aziende stanno iniziando ad assumere talenti con competenze in informatica quantistica, per identificare e applicare soluzioni che sfruttino le nuove possibilità di questa frontiera *dell'information technology*. L'innovazione da sola non può sbloccare il pieno potenziale dell'informatica quantistica; i leader aziendali e tecnologici devono fare il salto ora o rischiano di rimanere indietro. Oggi istituzioni e aziende come Mitsubishi Chemical[9],

[7] https://xanadu.ai/press/xanadu-launches-first-public-cloud-deployed-computer-with-quantum-computational-advantage

[8] https://research.ibm.com/blog/next-wave-quantum-centric-supercomputing

[9] https://www.ibm.com/quantum/use-case/mitsubishi-chemical

Keio University[10], ExxonMobil, CERN[11], Daimler AG[12], Fraunhofer[13], il governo del Quebec[14] e il CNR[15] collaborano con grandi player internazionali come IBM per esplorare nuovi casi d'uso e future applicazioni quantistiche man mano che hardware e software continuano ad evolversi.

Dalla grande accelerazione che sta avendo questa tecnologia nasce la consapevolezza e la necessità per l'Italia di scegliere una sua via di preparazione all'adozione della computazione quantistica.

3.4. Introduzione alla sicurezza resistente agli attacchi quantistici

Il quantum computing non promette però solo di superare i limiti dell'attuale capacità computazionale; esso potrà costituire anche una potenziale minaccia, in particolare per gli attuali schemi crittografici. Sono infatti già noti alcuni algoritmi quantistici che potranno "rompere" gli strumenti con cui oggi proteggiamo i nostri dati. Fortunatamente questi algoritmi richiedono calcolatori molto più potenti di quelli che abbiamo oggi a disposizione, ma vista l'importanza di questo tema è fondamentale muoversi rapidamente.

Nel luglio del 2022, dopo un processo di valutazione di oltre sei anni, sono stati selezionati[16] 4 nuovi algoritmi di crittografia resistenti agli attacchi che

[10] https://research.ibm.com/blog/japan-quantum-system-one
[11] https://www.ibm.com/case-studies/cern/
[12] https://www.wsj.com/articles/mercedes-enlists-quantum-computing-to-build-a-better-electric-vehicle-battery-11551134576
[13] https://research.ibm.com/blog/fraunhofer-quantum-system-one
[14] https://www.ibm.com/easytools/runtime/hspx/prod/public/X0027/PortalX/it/it/page/pageTemplate?s=78c374df5c884363b46454a5ffefb5d9&c=76420e94c84e47f3b751b178a0b8d806
[15] https://www.ibm.com/easytools/runtime/hspx/prod/public/X0027/PortalX/page/pageTemplate?s=78c374df5c884363b46454a5ffefb5d9&c=45db6b41bfaa45fdab83243a1443b36c
[16] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

potrebbero provenire dai computer quantistici del futuro. Per molte tipologie di dati è ancora presto pensare ad un cambio immediato degli schemi crittografici, ma è fondamentale cominciare a prepararsi adesso per l'arrivo della futura minaccia.

La prima attività da svolgere da parte di tutte le istituzioni e aziende che gestiscono dati sensibili è la mappatura di tutti gli schemi crittografici in utilizzo.

Il 4 maggio del 2022 il presidente degli Stati Uniti, Joe Biden, ha inviato un memorandum[17] a tutte le agenzie governative statunitensi chiedendo di eseguire l'inventario dei modelli crittografici in uso per proteggere i dati.

Il passo successivo, prima dell'implementazione degli algoritmi selezionati dal NIST, sarà lo sviluppo di processi per poter cambiare rapidamente gli schemi crittografici in uso quando richiesto. Questa tipologia di processi passa sotto il nome di Crypto Agility e garantirà la rapidità e la flessibilità nell'adeguamento degli schemi crittografici qualora lo sviluppo della tecnologia quantistica dovesse avere uno sviluppo inaspettato.

Da fine settembre del 2022, la GSMA (Global System for Mobile Communication Association) insieme a Vodafone e IBM stanno operando per identificare i passaggi chiave necessari per l'implementazione di tecnologie a sicurezza quantistica in infrastrutture di telecomunicazioni critiche, come le reti alla base dell'accesso a Internet e la gestione dei servizi pubblici [18].

3.5. Introduzione alla sicurezza delle comunicazioni quantistiche[19]

La protezione delle comunicazioni sta assumendo un valore sempre più strategico per la sicurezza e lo sviluppo, non solo tecnologico, di un paese; i recenti fatti di cronaca relativi al crescente numero di cyberattacchi dimostrano

[17] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[18] https://www.gsma.com/newsroom/press-release/gsma-ibm-and-vodafone-establish-post-quantum-telco-network-taskforce/

[19] *Per approfondimenti, si veda il White Paper dedicato "Tecnologie Quantistiche per la sicurezza delle Comunicazioni Digitali".*

che dotarsi di adeguati sistemi di protezione dei dati è una priorità non più differibile.

Esistono diversi livelli di sicurezza nelle comunicazioni e conseguentemente diversi sistemi di protezione; tuttavia, nessun sistema crittografico è completamente sicuro essendo esso basato sulla (supposta) difficoltà da parte di un avversario in possesso di determinate risorse computazionali di risolvere i problemi matematici sottostanti allo schema crittografico in questione-e, almeno in linea di principio, può essere violato, se si ha accesso ad una potenza di calcolo sufficientemente elevata, che potrebbe essere resa disponibile da sistemi di computazione quantistica.

La crittografia quantistica si pone quindi su un piano diverso rispetto ai sistemi classici perché è in grado di offrire una sicurezza assoluta nella generazione della chiave crittografica utilizzata per criptare e decrittare i messaggi: è questo un elemento innovativo nella sicurezza delle comunicazioni poiché viene offerta la possibilità di utilizzare chiavi di cifratura basate su fotoni, in virtù delle proprietà quantistiche dei fotoni stessi poiché- qualunque intervento esterno inevitabilmente modifica il loro stato, e tale modifica può essere rivelata dal mittente e dal destinatario.

Nel processo di generazione quantistica della chiave, mittente e destinatario si scambiano infatti singoli pacchetti di luce (i fotoni) in ciascuno dei quali è codificato un bit della chiave. Lo scambio dei fotoni è intrinsecamente sicuro perché, in virtù delle proprietà quantistiche dei fotoni stessi, qualunque intervento esterno volto a leggere e copiare l'informazione in essi codificata inevitabilmente modifica il loro stato, e tale modifica può essere rivelata dal mittente e dal destinatario. Se ciò accade, il processo di generazione della chiave viene interrotto, la sicurezza del canale viene ripristinata, per poi riprendere il processo, a conclusione del quale il messaggio criptato può essere inviato in modo completamente sicuro.

Uno use case applicabile in questo contesto può consistere nella creazione di una rete di comunicazione quantistica che collega soggetti pubblici, creando un canale sicuro di comunicazione (con tecnologia quantistica) da utilizzare a livello governativo su tratte di in fibra dedicate.

L'introduzione di tali reti è già oggetto di investimenti a livello Europeo attraverso il programma EuroQCI e il suo segmento spaziale gestito da ESA, denominato SAGA. Notare che la comunicazione quantistica è a uno stadio di

maturità nettamente superiore, con soluzioni commerciali disponibili su scala metropolitana[20].

Una comunicazione sicura è quindi di importanza fondamentale a livello governativo, militare, economico; per questa ragione le più grandi potenze mondiali (soprattutto Cina, USA, Canada, Regno Unito, Unione Europea) hanno avviato importanti programmi per lo sviluppo della comunicazione sicura con tecnologia quantistica.

Più in dettaglio, ci riferiamo a:

- *Quantum Cybersecurity*: per superare gli attuali sistemi in ambito sicurezza con Encryptor quantistici, generatori di numeri casuali quantistici, generatori di chiavi quantistiche, e in ambito comunicazioni criptate con la Quantum Key Distribution.
- *Quantum Blockchain*: soluzioni post quantistiche con algoritmi a chiave simmetrica con aumentata dimensione delle chiavi, eliminazione hashing crittografico e utilizzo di nuove strategie, nuovi algoritmi post-quantistici per le chiavi pubbliche.

[20] https://www.ey.com/en_uk/news/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services

4. AMBITI DI APPLICAZIONE DEL QUANTUM COMPUTING

I principali ambiti di applicazione della computazione quantistica sono:

- L'analisi dei processi fisici e chimici in particolare nei campi della chimica quantistica, scienza dei materiali e fisica delle alte energie.
- La simulazione di scenari con applicazioni in molti ambiti quali quello finanziario, geologico e il settore delle previsioni metereologiche.
- I processi di ottimizzazione che sono trasversali ad ogni ambito produttivo: dall'ottimizzazione delle rotte commerciali alla supply chain, dalla distribuzione della rete elettrica all'ottimizzazione di un portafoglio finanziario, dal dimensionamento ottimo di una rete di telecomunicazioni all'ottimizzazione nell'allocazione delle risorse nei data center, nella gestione del traffico dati e, in generale, dei consumi energetici di rete.
- Gli algoritmi di intelligenza artificiale e in particolare nell'ambito del *deep learning,* i cui modelli prevedono milioni di parametri che richiedono settimane o mesi per il loro addestramento. Il quantum AI si pone, infatti, l'obiettivo di superare i limiti attuali dei computer tradizionali, offrendo performance anche migliori di quelle ottenute con le tradizionali CPU e le moderne GPU.

Come è possibile vedere dalla figura 4 sotto riportata, questi ambiti sono trasversali a molti settori industriali che potranno beneficiare in vario modo dell'applicazione della computazione quantistica ai propri processi di business e di servizio al cittadino.

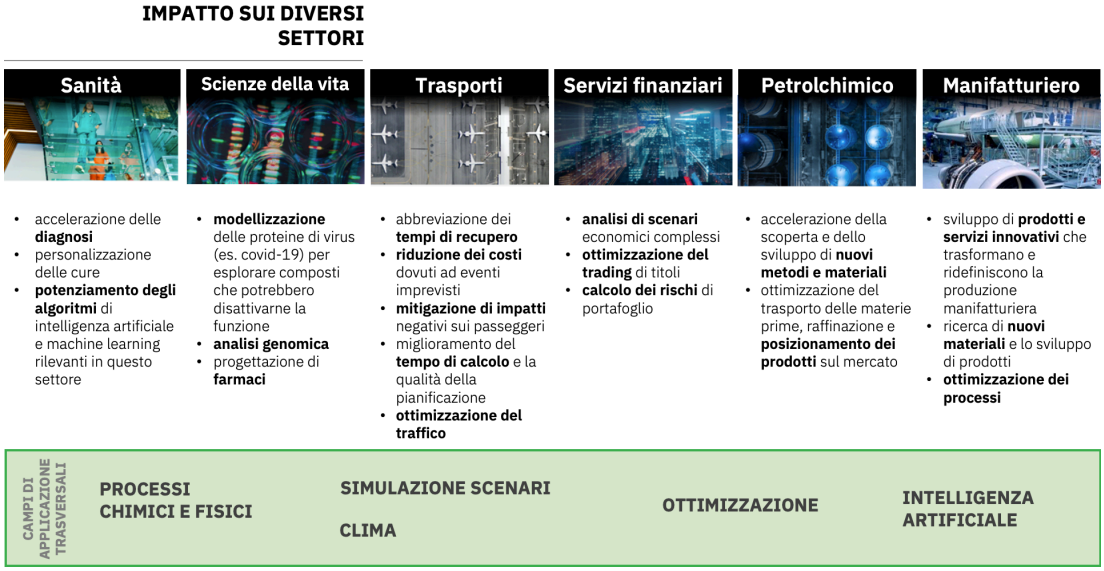


fig.4 Impatti potenziali Vs Settori economici[21]

Di seguito forniamo esempi dettagliati per alcuni dei principali settori industriali e aree di applicazione.

Il settore dei servizi finanziari ha storicamente applicato con successo vari modelli tratti dallo studio della fisica per aiutare a risolvere alcuni dei suoi problemi più spinosi. L'applicazione della tecnologia quantistica ai problemi finanziari, in particolare quelli che si occupano di incertezza e ottimizzazione vincolata, promette di portare grande vantaggi a questo settore. Le capacità di ottimizzazione del calcolo quantistico possono consentire ai gestori degli investimenti di migliorare la diversificazione del portafoglio, ribilanciare gli investimenti e semplificare in modo più conveniente i processi di regolamento delle negoziazioni per portafogli di grandi dimensioni. Le innovazioni nelle capacità di calcolo quantistico possono inoltre accelerare le simulazioni di scenari di rischio e migliorarne la precisione.

JPMorgan Chase, ad esempio, già da alcuni anni collabora con i principali fornitori di tecnologia per lo sviluppo di metodologie di calcolo quantistico per

[21] Fonte: IBM

la modellazione finanziaria, tra cui la determinazione del prezzo delle opzioni e l'analisi del rischio.

Anche per la segmentazione dei clienti e la modellazione delle previsioni, l'informatica quantistica potrebbe rappresentare un punto di svolta. Si prevede che le capacità di modellazione dei dati dei computer quantistici si dimostreranno superiori nel trovare modelli, eseguire classificazioni e fare previsioni che oggi non sono possibili a causa della complessità nell'analisi dei dati.

Nel settore ICT e Telecomunicazioni, l'integrazione dei quantum computing con High Performance Computing potrebbe consentire di risolvere in tempi più brevi problemi di ottimizzazione con vincoli molto complessi.

Alcuni esempi di tali problemi riguardano: pianificazione di rete, ottimizzazione nell'assegnazione dinamica di risorse di rete e servizi; ottimizzazione di flussi di traffico; potenziamento delle prestazioni dei sistemi di AI; classificazione di dati su spazi di grosse dimensioni, identificazione di pattern, o schemi, ricorrenti per applicazioni e servizi. In generale i benefici attesi sono:

- riduzione del TCO della rete ed aumento delle prestazioni: grazie all'utilizzo della computazione quantistica sarà possibile ottimizzare l'uso delle risorse di rete, i consumi energetici ed i costi operativi;
- aumento dei livelli di sicurezza nelle comunicazioni e nello scambio dati: grazie ai sistemi Quantum Key Distribution (QKD) e (Quantum Random Number Generation (QRNG) sarà possibile fornire servizi crittografia praticamente inviolabili in quanto basati sui paradigmi della fisica quantistica (per approfondimenti, si veda il par. 3.4);
- nuovi servizi e paradigmi di interazione e comunicazione, ad es. Quantum Security and Computing as a Service, evoluzione verso l'Internet Quantistica [22].

Nel settore sanitario, ci aspettiamo che l'uso dei computer quantistici in combinazione con i computer classici conferisca vantaggi sostanziali che l'informatica classica da sola non può offrire.

[22] Esempio: https://www.gruppotim.it/en/press-archive/corporate/2020/TIM-Quantum-computing-250220.html

Pensiamo per esempio alla ricerca medica: i dati sanitari come le informazioni provenienti da studi clinici, registri di malattie, cartelle cliniche elettroniche (EHR) e dispositivi medici hanno un tasso di crescita annuale del 36%. Con le tecnologie attuali non siamo ancora in grado di analizzare velocemente questa mole di dati destinata a diventare sempre più grande e modellizzare sistemi biologici in maniera efficace. Uno degli ambiti di applicazione è anche la medicina di precisione, che punta a identificare e spiegare le relazioni tra interventi e terapie, da un lato, e risultati, dall'altro, per fornire le migliori azioni mediche a livello individuale.

Tradizionalmente, la diagnosi delle condizioni di un paziente si basa fortemente sui sintomi riportati dal paziente e dai dati ottenuti dalle tecniche strumentali classiche, il che richiede molto tempo e si traduce in una diagnosi generica e in un trattamento associato che spesso fallisce. Negli ultimi anni, ci stiamo muovendo verso un approccio basato sulla medicina di precisione; il quantum computing ha il potenziale di facilitare e accelerare la transizione dalla medicina con approccio *one-size-fits-all* verso una medicina personalizzata per il singolo paziente e in base ai suoi obiettivi di salute. Inoltre, di recente, all'interno del processo diagnostico e di definizione del più adatto percorso terapeutico vengono inglobati anche i dati omici, caratterizzati da un elevatissimo numero di *feature* che interagiscono tra loro, portando ad interdipendenze, correlazioni e *pattern* che sono difficili da individuare e studiare con le tradizionali tecniche computazionali.

Il quantum computing ha anche il potenziale di rivoluzionare la ricerca e lo sviluppo di nuove molecole nell'industria farmaceutica. L'opportunità di velocizzare enormemente e rendere più efficienti le fasi di identificazione del target terapeutico, di progettazione del farmaco e dei test di tossicità, notoriamente dipendenti da un processo di *trial and error*, porterà ad un netto miglioramento della qualità di vita dei pazienti, permettendo di avere il giusto farmaco per il giusto paziente in tempi rapidi e in maniera più efficiente.

La Cleveland Clinic ha stretto una partnership con IBM nel 2021 per portare le capacità rivoluzionarie della computazione quantistica nelle mani di scienziati e professionisti nel settore sanitario.

Questa nuova tecnologia è destinata inoltre a diventare uno strumento chiave di trasformazione per il *settore manifatturiero.* Con il suo impatto previsto sullo sviluppo e la progettazione del prodotto, sui processi di produzione e sulle

attività della catena di approvvigionamento, potrebbe fornire un vantaggio decisivo a chi per primo ne sperimenterà l'utilizzo.

I computer quantistici saranno in grado di simulare le interazioni dei componenti all'interno di macchinari complessi, calcolando in modo più preciso e completo i carichi del sistema, i percorsi di montaggio, il rumore e le vibrazioni. Questa analisi integrata può ottimizzare la produzione dei singoli componenti nel contesto del sistema complessivo, riducendo i costi senza sacrificare le prestazioni.

L'informatica quantistica potrebbe aiutare a trovare nuove correlazioni nei dati e migliorare i modelli di classificazione oltre le capacità dell'informatica classica. Si prevede che la combinazione di calcolo quantistico e machine learning, nonché la sua applicazione all'ottimizzazione, avrà un impatto significativo nel settore manifatturiero in diverse aree.

Daimler, per esempio, sta lavorando sui processori quantistici per comprendere come l'informatica quantistica potrà far progredire lo sviluppo di nuovi materiali per le batterie dei veicoli elettrici e migliorare le tecniche di produzione automobilistica.

5. QUALE STRATEGIA ADOTTARE

Il quantum computing diventerà fondamentale per approcciare i problemi di complessità elevata.

La complessità computazionale di un problema è definita dal tempo necessario a un computer per risolvere un problema in relazione alla dimensione del problema stesso. Da questa definizione nascono le cosiddette classi di complessità, a seconda della crescita del tempo computazionale in relazione alla dimensione del problema: i problemi con crescita polinomiale, i problemi con crescita logaritmica, i problemi con crescita esponenziale, etc.

Il quantum computing permette di approcciare problemi con complessità proibitiva per i calcolatori classici, in particolare quelli di complessità esponenziale, sfruttando le proprietà di sovrapposizione degli stati, entanglement e interferenza, che permettono di osservare una *Practical Quantum Advantage* utilizzando anche algoritmi che consentono di rappresentare dati in maniera estremamente compatta e sviluppando anche algoritmi che possano processare ed elaborare i dati rappresentati nei qubits, come nel caso degli algoritmi di Grover.

Come accennato al par. 2, nel breve termine, si possono utilizzare i sistemi quantistici NISQ per sviluppare abilità e competenze. La commercializzazione e il successo delle applicazioni del sistema NISQ nei prossimi cinque anni saranno fondamentali per l'adozione continua e il finanziamento di iniziative a lungo termine. Sarà necessaria, a tal riguardo, l'individuazione di casi d'uso quantistici o simulati quantistici che possano contribuire alla creazione di valore aziendale, utilizzando circuiti poco profondi, con risultati dimostrabili e ripetibili.

L'ideazione delle prime iniziative di quantum computing creerà nuovi champion in grado di comprendere il contesto aziendale e le capacità necessarie per navigare in un ecosistema quantistico in rapida evoluzione.

Le aziende che cercano applicazioni di quantum computing per problemi rilevanti dovranno scoprire nuovi approcci algoritmici e riprogettare le applicazioni in un contesto quantistico.

È probabile che le imprese che investono nella scoperta di nuovi approcci algoritmici per un contesto quantistico scoprano modi nuovi, innovativi e potenzialmente dirompenti per risolvere gli stessi problemi in un contesto classico.

La standardizzazione dei modelli di delivery come il quantum computing as a Service (QCaaS) sta emergendo come modello standard tra i principali fornitori di sistemi di quantum computing.

6. Use cases e Best practices

Nell'ambito del quantum computing, sta emergendo un importante spazio per sviluppare algoritmi e soluzioni specifiche.

Tra le aree tecnologiche più promettenti a tal riguardo, si rileva il *Quantum Machine Learning (QML):* per estrarre valore dai dati e dare supporto a soluzioni di business guidate dai dati in maniera più efficacemente rispetto a quanto avviene oggi; il *Quantum Optimization (QO*): algoritmi di ottimizzazione dinamica e lineare, ottimizzazione combinatoria quadratica e a variabili binarie flessibili, che uniti alla velocità di calcolo quantistico possono supportare problemi complessi; il *Quantum Simulation*: algoritmi di simulazione per analizzare le proprietà delle molecole e i comportamenti di reazioni chimiche utili per la messa a punto di nuovi materiali e farmaci.

Di seguito, inoltre, alcuni modelli, metodologie e applicazioni.

6.1. Quantum NLP

All'interno del filone Intelligenza Artificiale e in maniera abbastanza trasversale a molti dei domini di applicazione suindicati, si sta sperimentando l'applicazione dell'informatica quantistica sui modelli di apprendimento automatico basati sull'analisi del linguaggio naturale (NLP, Natural Language Processing). Ovvero quella tecnologia che mira ad estrarre, riconoscere e aumentare il contributo informativo nascosto nelle parole che compongono un documento non strutturato (tipicamente privo di un qualsiasi schema organizzativo precostituito). L'NLP è lo strumento attraverso il quale, ad esempio, gli assistenti vocali interpretano le richieste e sono in grado, nelle implementazioni più all'avanguardia, di sostenere una conversazione come se stessimo interagendo con una persona. Ebbene, questa capacità, sempre più sofisticata, di rendere l'interazione uomo-macchina il più naturale possibile, è accompagnata da un livello parimenti crescente di complessità secondo il quale, per addestrare i nuovi modelli di reti neurali a riconoscere il linguaggio, è richiesta l'elaborazione di tera e tera di dati (l'intera versione multilingue di Wikipedia), con conseguente dispendio di tempo, risorse e calcolo.

Il Quantum NLP nasce dalla constatazione che il modello del qubit, la sovrapposizione e la possibilità di codificare diversi stati macchina in una sola

informazione, ben si adattino alla rappresentazione del contributo delle parole all'interno di una frase, e la capacità di formalizzare contemporaneamente, negli stati quantistici, sia le strutture sintattiche, che il significato semantico di un testo. In tal senso, si stanno conducendo diversi esperimenti su determinate funzionalità dell'NLP come: l'Information Extraction, il Question & Answering e la Sentiment Analysis, adottando approcci differenti. Si parte da quelli teorici, che mirano a dimostrare l'efficacia dell'utilizzo della QRAM (Quantum RAM) nell'esecuzione dei modelli di implementazione attuale di AI, per passare a quelli che utilizzano modelli di rappresentazione a stati quantistici su elaboratori di calcolo con hardware tradizionale, e finire con quelli eseguiti direttamente su elaboratori di calcolo quantistico (hardware NISQ), ma che oggi soffrono ancora di elevato rumore.

A prescindere dalle strategie, tutte hanno dimostrato che attraverso l'uso di QNLP, sarà possibile svincolarsi dalla dipendenza di grandi insiemi di dati e da modelli che richiedano una enorme quantità di parametri. Restano tuttavia ancora aperte diverse questioni sia dal punto di vista teorico, sulla capacità di creare descrizioni formali efficaci del linguaggio, che dal punto di vista applicativo, sulla possibilità di spingere QNLP alla risoluzione di problemi di ambiguità e correlazioni nel testo, su dati reali (e non solo a livello di benchmark), che rappresentano ancora oggi le sfide più difficili dell'NLP. Insomma, siamo all'inizio, ma le premesse sembrano essere rivoluzionarie.

6.2. Variational Algorithms

Il campo delle quantum optimization (QO) offre applicazioni pratiche in differenti campi: da problemi strettamente industriali (come production planning, localizzazione, ottimizzazione delle risorse e del traffico in una rete di Telecomunicazioni) a organizzativi (come il Routing, la schedulazione dei turni di lavoro). Tra le varie tecniche di QO, una tra tutte sta prendendo piede come una tra le più funzionali e con risultati tangibili: i variational algorithms (come il Quantum Approximate Optimization Algorithm) sfruttano una collaborazione tra i sistemi classici e quelli quantistici, macinano i dati forniti da input in soluzioni ottimali, facendoli passare in un "loop feedback" tra le due risorse.

Fornire algoritmi basati su queste tecniche e funzionali per le grandi industrie, permetterebbe alle stesse di: migliorare la loro produzione; diminuire l'emissione di carbonio ottimizzando i path di consegna e trasporto materiali;

migliorare la life-work balance trovando turni di lavoro migliori per i propri dipendenti; migliorare l'allocazione di risorse di rete e di banda in una rete di telecomunicazioni e ottimizzare il *routing* del traffico dati.

La corsa all'ottimizzazione è all'ordine del giorno nella società: utilizzare un acceleratore quantistico migliorerebbe tecniche già a noi conosciute, tenuto conto che il vantaggio del quantum computing in questo ambito è quello di analizzare un campo di problemi e di soluzioni ben maggiore rispetto alla loro controparte classica, fornendo risultati in tempo uguale o addirittura minore.

6.3. Il Deep Reinforcement Learning

Il *deep force learning* diventa la base metodologica di calcolo del nuovo paradigma che presenta un nuovo framework di controllo quantistico generato utilizzando questa tipologia di apprendimento, la quale permette di incapsulare in un'unica funzione di *cost control* i diversi aspetti di controllo quantistico. Può essere usato per la compilazione dei circuiti quantistici e consente inoltre di sfruttare le capacità di *quantum-as-a-service* per convalidare ipotesi che coinvolgono il Machine Learning (ML) quantistico per ridurre al minimo i rischi e massimizzare l'accessibilità delle risorse di calcolo quantistico.

7. Lo sviluppo delle competenze e le proposte di policy per l'adozione della computazione quantistica in Italia

Lo sviluppo di algoritmi e applicazioni sui computer quantistici non è un'attività semplice da realizzare: la programmazione quantistica è infatti una rivoluzione e non una semplice evoluzione dei modelli di programmazione adoperati fino ad oggi.

La sfida del quantum computing, si giocherà quindi anche sulla capacità di sapere utilizzare in modo efficiente ed efficace i sistemi hardware che verranno sviluppati.

La possibilità di possedere il know-how necessario allo sviluppo di applicazioni su computer quantistici rappresenterà un vantaggio competitivo strategico per lo sviluppo in campo scientifico ed industriale.

In tale ottica, è fondamentale pianificare azioni di formazione mirate sia a sviluppare nuove competenze per coloro che già lavorano nell'ambito delle tecnologie dell'informazione, sia alla creazione di nuovi profili professionali espressamente orientati alla programmazione quantistica.

I nuovi profili dovranno essere in grado di definire, consigliare, attivare e sviluppare progetti basati su tecnologie quantistiche, oltre a comprenderne i concetti fondamentali per gestire i progressi e il know-how tecnico utile per stare al passo con tecnologie in continua evoluzione.

In particolare, all'alba di questa nuova fase tecnologica, sta nascendo dal mondo industriale una richiesta di nuovi profili quali:

- *Il Quantum Scientist*, che ha profonde capacità scientifiche ed è un esperto di teoria e tecnologia quantistica. È una figura determinante sia per affrontare problemi fondamentali, come la mitigazione del rumore e il design di dispositivi e algoritmi efficaci, sia nei settori verticali di applicazione, lì dove è richiesta una conoscenza robusta dei modelli e metodi computazionali basati sulla meccanica quantistica.
- *Il Quantum Engineer*, che ha una profonda e dettagliata comprensione della tecnologia quantistica, sia dal punto di vista informatico che dal punto di vista dell'ottimizzazione hardware, ed è in grado di configurare e progettare soluzioni valide ed efficienti per problemi specifici. Deve dialogare con il Quantum Scientist ed essere in grado di comprendere i risultati e le scoperte principali che avvengono in fase di ricerca di soluzioni.

Un Quantum Engineer può essere specializzato in un campo della conoscenza o della tecnologia quantistica, ma deve essere in grado di collegare e combinare diverse tecnologie quantistiche con tecnologie convenzionali per realizzare progetti globali che risolvano situazioni complesse. È richiesta, per questa figura, una padronanza di base della meccanica quantistica, dell'elettronica, dei sistemi fotonici, delle nanotecnologie e delle tecnologie dell'informazione.

- *Il Quantum Developer*, che è l'equivalente di un programmatore di sistemi o di uno sviluppatore di applicazioni. È una figura professionale con le conoscenze necessarie per sviluppare un programma che funzioni su un simulatore o un processore quantistico. Questa figura professionale, oltre a conoscere i concetti fondamentali della meccanica quantistica, deve possedere dimestichezza con lo sviluppo software (quantistico e classico) e avere solide basi di teoria dell'informazione.

Per soddisfare queste richieste, ecco le proposte di alcuni interventi cardine:

a) È fondamentale iniziare subito a lavorare e completare la missione 4 del PNRR, in un contesto di pieno scambio di competenze tra università e impresa con l'ipotesi di creare dei centri di competenza dedicati alle tecnologie più all'avanguardia

b) Dare forma ai piani didattici delle facoltà STEM o modificarli, per accogliere nuovi contenuti che consentano la creazione dei suddetti profili. Infatti[23] si potrebbe presto verificare una situazione paradossale, con un mercato e una industria pronti a investire nelle *quantum technologies*, senza però avere una forza lavoro formata e consistente in grado di sopperire alla domanda.

   Tuttavia, nonostante in Italia siano attualmente in crescita varie realtà accademiche che si pongono l'obiettivo di dare una prima formazione sul quantum computing e/o sulla quantum communication, percorsi formativi specifici su figure professionali come quelle sopra elencate sono ancora di là da venire.

c) Creare sinergie stabili tra pubblico e privato in grado di coniugare "*ab initio*" gli aspetti scientifici e metodologici del quantum computing con

[23] Secondo un recente studio di McKinsey

gli aspetti applicativi di interesse industriale. Strumenti come i dottorati industriali e, ancor di più, la costituzione di laboratori congiunti e l'interazione con network internazionali tematici (e.g. IBM Quantum Network) possono essere i fattori abilitanti per uno sviluppo significativo delle competenze della programmazione quantistica orientate alle grandi sfide industriali.

Inoltre, andranno valorizzate le iniziative già in atto volte a favorire tale collaborazione*:*

a) la Commissione Europea ha stanziato un pacchetto consistente di investimenti in ricerca e sviluppo sul quantum computing, sia nel pubblico che nel privato, per portare l'intera Unione a un livello di maturità tecnologica al pari di altri partner internazionali. Inoltre, molte imprese nazionali e internazionali stanno investendo e mostrando un crescente interesse nell'utilizzo delle tecnologie quantistiche per risolvere problemi ad alto impatto relativi al proprio "core" business (es. l'ottimizzazione di batterie elettriche, la scoperta di nuovi composti chimici per l'industria farmaceutica, e l'intelligenza artificiale).

b) Il Centro Nazionale HPC, attraverso Cineca ha sottoposto una richiesta di finanziamento alla JV europea High Performance Computing Joint Undertaking (Euro HPC JU) per cofinanziare un Quantum Computer da installare sul suolo italiano.

   Sul finire del 2022, la Euro HPC JU ha annunciato la selezione di sei siti in Repubblica Ceca, Germania, Spagna, Francia, Italia e Polonia che ospiteranno i primi computer quantistici europei. Queste nuove tecnologie all'avanguardia saranno integrate in loco nei supercomputer esistenti e dovrebbero essere disponibili nella seconda metà del 2023[24]

   Leonardo ha comunicato il proprio supporto a questa iniziativa e conta di utilizzare le risorse per computazioni ibride Quantum-HPC. Infatti sono stati allestiti i Leonardo Labs: uno di essi è focalizzato sulle tecnologie quantistiche ed uno sull'HPC.

[24] https://fasi.eu/en/news-2/81-funding/news/25055-eu-deploys-first-quantum-technology-in-six-sites-across-europe.html)

c) Il progetto per dotare l'Italia di una rete di supercomputer a mezzo del consorzio guidato dall'INFN, l'Istituto nazionale di fisica nucleare, con Cineca e IIT-Istituto italiano di tecnologia con una cordata che comprende centri di ricerca, tra cui appunto INFN che ne è capofila, e 15 grandi partner industriali (tra i quali figurano anche Autostrade, FS, Engineering, ThalesAlenia, Fincantieri, Terna, Sogei, Humanitas, Upmc, Fiu, iFab, Intesa Sanpaolo e Unipol Sai) nell'ambito del bando PNRR del Ministero dell'Università e della Ricerca, relativo alla creazione di cinque centri nazionali dedicati alla ricerca di frontiera in ambito "digitale" che afferiscono ai settori mobilità, agritech, medicina, biodiversità e supercalcolo".

d) Eni, che gestisce uno dei più potenti supercomputer privati al mondo, con sede nel Green Data Center di Eni a Ferrera Erbognone (PV), e PASQAL hanno annunciato l'avvio di una collaborazione per lo sviluppo di soluzioni HPC di informatica quantistica di ultima generazione per il settore energetico

   L'applicazione della tecnologia quantistica al settore energetico è uno strumento innovativo che potrebbe accelerare ulteriormente la transizione energetica in termini di aumento di efficienza a riduzione netta delle emissioni di GHG.

e) Neva SGR, società del Gruppo Intesa Sanpaolo controllata al 100% da Intesa Sanpaolo Innovation Center, ha concluso tramite il proprio Fondo Neva First un investimento in Classiq, società israeliana leader nell'innovativo ambito del quantum computing. La collaborazione è destinata a concretizzare gli investimenti in quantum computing nei settori dei servizi finanziari, bancari e assicurativi.

f) La realizzazione della combinazione di aree quali:

   - Quantum Sensing per PNT (es. clocks)
   - Quantum Imaging (es. sistemi "seeing behind the corner")
   - Quantum Networks (anche su scala continentale facendo leva su Euro QCI)

   con l'obiettivo di costruire una filiera che va dall'acquisizione del dato (Imaging +PNT sensing), al suo trasferimento in modalità sicura (Quantum Networks su larga scala), fino al suo processamento (quantum

computing), che viene sviluppato congiuntamente dai due laboratori. Il tutto sfruttando al meglio le potenzialità del "Quantum Tool".

g) L'utilizzo di tecnologie immediatamente disponibili come il *quantum annealing* e le attività di sviluppo, in ottica *quantum ready,* su algoritmi nei due principali modelli universali di computazione (*gate-based* e *measurement based*) coordinate da Leonardo.

In conclusione, affinché la computazione quantistica diventi nel breve periodo uno strumento efficace per la risoluzione di problemi complessi sia in ambito scientifico che industriale, non si può prescindere dal pianificare e realizzare iniziative di sistema volte alla formazione e allo sviluppo di nuove competenze in questo settore.

Inoltre, la scommessa sullo sviluppo di un ecosistema pubblico-privato, che veda il coinvolgimento non solo degli attori che sviluppano tecnologie ma anche dei grandi utenti professionali nazionali e del mondo bancario, dovrà essere quel valore aggiunto in grado di garantire, "by design", una ricaduta reale sul sistema Paese per competere a livello internazionale.

Con l'obiettivo di disporre di un quadro informativo il più possibile completo e accessibile, appare opportuno che i *policy makers* siano sufficientemente informati e consapevoli di tutti profili relativi a questo tema e alle attività già in corso.

Andrebbe, valutata l'opportunità di svolgere un'indagine conoscitiva in sede parlamentare e in altra sede deputata più consona, che potrebbe servire ad approfondire la tematica grazie alle audizioni di esperti, tecnici e aziende e fare insieme il punto della situazione, del contesto tecnologico e industriale e delineare le prospettive del settore.

8. Conclusioni

Come visto, lo sviluppo di un'industria quantistica nazionale sostenibile presuppone l'esistenza di un ecosistema quantistico attivo e vibrante che si forma attraverso le strette interazioni cicliche tra quattro componenti essenziali:

1. *Ricerca e sviluppo* che spinge i limiti dell'informatica quantistica sia dal punto di vista della creazione di tecnologie per l'industria sia dall'utilizzo dell'informatica quantistica come strumento per la ricerca fondamentale compreso lo sviluppo di algoritmi e applicazioni.
2. *Formazione professionale* per una forte forza lavoro che sviluppa nuove soluzioni per problemi aziendali complessi e consente il miglioramento delle competenze e la riqualificazione della forza lavoro esistente per essere pronta per la tecnologia quantistica.
3. *Settori industriali* il cui coinvolgimento può essere suddiviso in tre direttrici:
    - industrie che si impegnano a utilizzare l'informatica quantistica per migliorare i loro prodotti,
    - industrie che vogliono contribuire alla costruzione dei sistemi quantistici e della catena di fornitura tecnologica (elettronica, amplificatori, criogenia, ecc.),
    - industrie che possono contribuire a costruire il futuro digitale che sarà un insieme di dati, informatica e comunicazione sia classici che quantistici.
4. *Servizi e infrastrutture quantistiche* che portano la tecnologia del quantum computing nell'ecosistema con una roadmap che identifica il percorso da seguire per il miglioramento continuo.

Ogni componente rafforza le altre: il coordinamento nel loro sviluppo è quindi importante per un ecosistema di successo.

Oggi l'accesso ai calcolatori quantistici è possibile attraverso il cloud, ma molte nazioni, come la Germania e il Giappone, hanno già stretto accordi per disporre di computer quantistici sul suolo nazionale; questa scelta garantirà maggior controllo per sfruttare questa tecnologia a supporto degli obiettivi del Paese e la possibilità di formare professionalità che siano in grado di lavorare direttamente su queste nuove soluzioni.

A livello Italia, dal 1° febbraio 2022 i ricercatori del CNR possono accedere ai processori quantistici più potenti al mondo. Oggi le ricerche si stanno conducendo sui sistemi attuali, ma guardano già al rilascio di Condor di IBM, il processore da 1.121 qubit previsto per il 2023; per alcuni algoritmi questa nuova tecnologia sarà profondamente vantaggiosa e industrie e università potranno quindi finalmente utilizzare questo strumento in produzione.

L'Italia ha davanti a sé una grande sfida e un importante ruolo da giocare sul quantum computing che gli permetterà di prendere il meglio da questa tecnologia per renderlo funzionale agli obiettivi di crescita del paese. Da una parte, le nostre università formano scienziati di prim'ordine, anche nell'ambito della fisica quantistica, e hanno già attivato corsi di informatica quantistica e gruppi di ricerca per il calcolo quantistico. Dall'altra parte le aziende italiane si interessano attivamente, collaborano, si relazionano con le università e creano un ecosistema.

Tuttavia, per coltivare una nuova generazione pronta ad affrontare le sfide dei calcolatori quantistici, è opportuno potenziare l'offerta formativa anche nelle scuole superiori, utilizzando strumenti grafici di più immediata comprensione che semplifichino alcune nozioni e comincino a introdurre la meccanica quantistica ad una platea più ampia.

Per catalizzare queste iniziative, all'estero sono stati fondamentali i fondi pubblici, che in Italia sono arrivati grazie al PNRR.

Il 2023 diventa quindi una reale e severa deadline entro cui l'Italia può diventare pronta ad utilizzare la computazione quantistica: è una sfida che riguarda tutti - università, istituzioni, imprese, centri di ricerca, startup e giovani –e sarà più semplice da vincere se affrontata assieme.