QUANTUM FINANCE

una panoramica delle possibilità attuali e prospettive future

cdp

CONTENTS

EXECUTIVE SUMMARY

Il termine Quantum Computing identifica un insieme di tecnologie hardware e di approcci algoritmici in grado di sfruttare le dinamiche uniche della meccanica quantistica al fine di ottenere dei vantaggi computazionali.

Negli ultimi anni si è osservata una crescita sempre più rapida e diversificata nella ricerca e nello sviluppo di approcci quantistici, prospettando un impatto a lungo termine potenzialmente rivoluzionario sul mondo delle tecnologie che ci circondano. La gamma di applicazioni di tali sviluppi abbraccia mondi estremamente eterogenei fra loro, dalle tecnologie alla base delle comunicazioni fino a quelle per l'analisi avanzata dei dati.

Da questo punto di vista, il settore finanziario risulta essere tra i primi campi di applicazione del Quantum Computing. La ragione di ciò risiede nella complessità computazionale intrinseca dei problemi della finanza: attività ordinarie del settore come l'ottimizzazione periodica dei portafogli o il trading richiedono infatti l'analisi di numerose variabili, spesso legate da relazioni complesse, da svolgersi nel minor tempo possibile. È proprio in questo senso che le potenzialità dei dispositivi quantistici, in grado di ridurre sensibilmente tempi e passaggi di calcolo, suscitano sempre maggiore interesse.

L'emergere delle potenziali capacità degli approcci quantistici rappresenta sempre più un punto di interesse anche sul fronte degli investimenti pubblici e privati. A titolo d'esempio è possibile citare i seguenti fatti:

- nel 2022 l'Unione Europea ha collocato complessivamente l'equivalente di circa 7 miliardi di dollari statunitensi che vanno a sommarsi ai circa 1,9 miliardi di dollari di finanziamenti stanziati dal governo degli Stati Uniti l'anno precedente. A questi si aggiungono un altro miliardo di dollari dal Canada. Infine, l'investimento pubblico totale annunciato dalla Cina di 15,3 miliardi di dollari risulta il più alto al mondo[1][2];
- gli impegni sia pubblici sia privati hanno raggiunto il totale di 35,5 miliardi di dollari, elevando il settore ad un nuovo livello di maturità rispetto al passato e dimostrando una nuova diffusa consapevolezza delle potenzialità legate all'applicazione della tecnologia[3].

La rilevanza dei dati sopracitati emerge soprattutto confrontando gli importi investiti con quelli degli anni precedenti. A tal proposito, si pensi a come gli investimenti privati nel solo 2021 abbiano raggiunto un totale di 3,2 miliardi di dollari contro i 5,5 dell'intero decennio precedente[4]. Il crescente interesse, da un lato, e la relativa progressione dei finanziamenti dall'altro, hanno favorito lo sviluppo di nuovi approcci tecnologici di cui anche il settore dei servizi finanziari può beneficiare.

Nella redazione del presente lavoro, Cassa Depositi e Prestiti ha ritenuto di avvalersi del contributo di Intesa Sanpaolo, considerato il ruolo di rilievo e la competenza nel contesto dell'adozione e sperimentazione delle tecnologie quantistiche in ambito finanziario, e del supporto di Data Reply.

Il documento intende approfondire le tecnologie quantistiche, il relativo stato dell'arte e quali, fra queste, risultano essere applicabili sin da ora nel contesto finanziario. In questo senso vengono presentati quelli che sono i concetti di base per la comprensione e l'applicazione della tecnologia per poi introdurre alcuni dei principali problemi di ottimizzazione e analisi finanziaria che, richiedendo un significativo carico computazionale, ben si prestano all'adozione di approcci quantistici. Sono, quindi, comparati approcci classici e quantistici per la risoluzione degli stessi e di ulteriori problemi per rilevarne le sostanziali differenze.

Senza alcuna pretesa di esaustività, agli argomenti citati si aggiunge un'analisi dell'impatto che queste tecnologie avranno sulla cybersecurity e sulle strategie da attuare per prepararsi a mitigare la possibile minaccia rappresentata dal Quantum Computing.

In conclusione, emerge dal lavoro come le potenziali ripercussioni su use case estremamente diversificati e i benefici già rilevabili in diversi contesti conducano alla necessità di acquisire competenze e sviluppare know-how su una tecnologia che a tutti gli effetti si candida ad avere una portata applicativa rivoluzionaria, in particolare nel settore dei servizi finanziari.

1 https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf

2 https://www.weforum.org/press/2022/01/first-quantum-computing-guidelines-launched-as-investment-booms/

3 Dati basati su dati pubblici di investimento registrati su PitchBook, gli importi reali sono probabilmente superiori.

4 https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf

SINTESI DEL CONTENUTO

Il presente documento è articolato in tre sezioni principali.

La prima si configura come una generale Introduzione al Quantum Computing. Questa risulta infatti necessaria non solo per avere una panoramica sulle principali tecnologie hardware attualmente in via di sviluppo, ma anche per avere una comprensione più dettagliata di come questo approccio, basato sulla meccanica quantistica, risulti altamente innovativo. Infine, viene presentato un quadro sistemico dello stato dell'arte del mercato e della ricerca.

La seconda sezione si concentra sul confronto tra le metodologie classiche e i possibili approcci quantum per la risoluzione di problemi di rilievo nel contesto finanziario come la Portfolio Optimization, l'Option Pricing, la Credit Risk Analysis e la Fraud Detection. Sono paragonate una serie di metodologie classiche e quantistiche volte alla risoluzione degli stessi problemi, in modo da evidenziarne le sostanziali differenze e compararne le performance in termini computazionali.

Nella terza e ultima sezione, si propone un'analisi degli impatti che questa tecnologia avrà nella comunicazione sicura delle informazioni. La capacità di calcolo promessa dagli hardware quantistici ha la potenzialità di violare alcuni dei più diffusi protocolli di crittografia attualmente in uso. Si presenta, dunque, una panoramica degli algoritmi crittografici classici e del rischio a cui saranno esposti nell'era post-quantum. Successivamente si esplorano le più promettenti alternative quantum-safe e si delinea una possibile rotta per la gestione della sicurezza delle informazioni in contesti di enti pubblici e privati.

In sintesi, il presente documento si pone l'ambizioso scopo di fare da tramite tra gli approcci computazionali classici, più efficaci e diffusi, degli ultimi decenni e quelli quantum-based, soprattutto in riferimento al contesto dei servizi finanziari. In questo modo, presentando le evidenze sui risultati che si sono raggiunti e si stanno raggiungendo, si lascia evincere la necessità di porre attenzione organica e sistemica sul tema Quantum Computing.

INTRODUZIONE AL QUANTUM COMPUTING

L'innovazione informatica degli ultimi decenni si è concentrata principalmente sulla continua miniaturizzazione e sui progressi nelle architetture hardware. Il progressivo avvicinarsi ad un limite fisico nella riduzione delle componenti a silicio, il quale potrebbe ostacolare la capacità di continuare a ottenere miglioramenti significativi in termini di prestazioni dei processori[5], ha spinto alcune delle grandi aziende ed enti di ricerca allo sviluppo di nuove alternative.

Una prima ragione che porta alla scelta del Quantum Computing al posto delle tecnologie classiche è dunque la possibilità di aprire la strada a miniaturizzazioni più avanzate rispetto a quelle che è possibile ottenere col silicio. Si consideri, a titolo d'esempio, che un qubit, l'unità di base del calcolo quantistico, può essere realizzato utilizzando anche un singolo atomo.

Una seconda motivazione legata all'introduzione del Quantum Computing deriva dalla teoria algoritmica che è alla base di questa disciplina, la quale offre, in potenza, vantaggi computazionali piuttosto significativi. In particolare, per alcune specifiche classi di problemi, esistono algoritmi quantistici in grado di ridurre decisamente il tempo di computazione rispetto ai corrispondenti algoritmi classici. Questa condizione prende il nome di "quantum advantage"[6].

Infine, un terzo aspetto chiave nell'approccio quantistico alla computazione è la potenziale riduzione del consumo energetico rispetto ai data center e alle tecnologie di calcolo tradizionali[7]. Il Quantum Computing offre la prospettiva di un minore impatto ambientale, quest'ultimo basato sul fatto che le operazioni quantistiche sono reversibili e quindi potrebbero, in linea teorica, non dissipare energia, al netto di quella utilizzata per garantire il controllo e la stabilità del sistema.

In questa prima sezione vengono introdotti i principali aspetti legati al mondo del Quantum Computing, dalle possibili implementazioni fisiche dei sistemi di qubit ai potenziali impatti sull'industria dei servizi finanziari.

5 Shalf, John. "The future of computing beyond Moore's law." Philosophical Transactions of the Royal Society A 378.2166 (2020): 20190061.

6 Zhong, Han-Sen, et al. "Quantum computational advantage using photons." Science 370.6523 (2020): 1460-1463.

7 Auffeves, Alexia. "Quantum technologies need a quantum energy initiative." PRX Quantum 3.2 (2022): 020101.

COS'È UN QUBIT

La risorsa fondamentale nel calcolo classico è il bit, il quale rappresenta la minima unità di informazione con solamente due valori possibili: 0 e 1. La capacità espressiva di un qubit, equivalente quantistico del bit, è invece di gran lunga maggiore. Ad esempio, immaginando di fissare un punto su una sfera che rappresenta il pianeta Terra, impiegando un singolo bit e fissato un orientamento, si è in grado al più di dire se ci si trova nell'emisfero Nord o in quello Sud, mentre con un qubit si possono ottenere esattamente le coordinate del punto, ovvero determinare la sua precisa posizione sul globo.

La formulazione matematica, qui omessa per semplicità, può essere descritta mediante una rappresentazione geometrica in cui lo stato del qubit è rappresentato come un punto su una sfera (la cosiddetta sfera di Bloch), come illustrato in Figura 1.

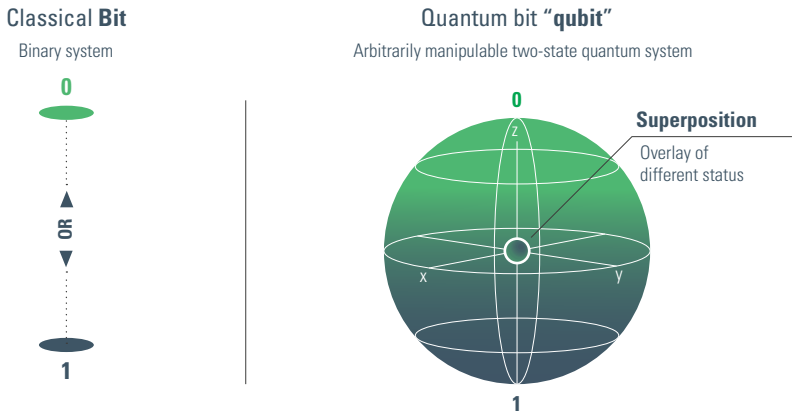

Figura 1: Rappresentazione di uno stato quantistico come punto sulla sfera di Bloch.[8]

Grazie a questa immagine, è possibile notare come il qubit abbia una capacità di rappresentazione delle informazioni del tutto diversa rispetto al classico bit.

DIFFERENZE RISPETTO ALLA COMPUTAZIONE CLASSICA

Muovendo dalla configurazione descritta nella precedente sezione, ossia la rappresentazione del qubit sotto forma di punto su di una sfera, esistono aspetti peculiari del calcolo quantistico, i quali vengono riportati nel seguente elenco:

- La superposition (o sovrapposizione) di stati
- L' entanglement
- L'effetto tunnel quantistico
- Il processo di misura (o osservazione)

Superposition: nell'informatica classica il bit, può assumere in un singolo istante temporale uno ed un solo valore: 0 oppure 1. Il qubit può invece trovarsi in una qualsiasi combinazione dei valori 0 e 1. Lo stato che il qubit assume in questa configurazione viene chiamato Superposition e se ne può trovare una raffigurazione in Figura 2.

Dal punto di vista intuitivo, questo concetto può essere meglio compreso attraverso il seguente esperimento mentale. Si prenda una moneta e la si lanci in aria. Prima di cadere, la moneta non è interamente testa, né croce, ma una combinazione di entrambi i possibili esiti del lancio. Si chiudano gli occhi e si aspetti che la moneta cada a terra. In questo momento la moneta può aver dato come risultato o testa o croce. La

8 Image from https://devopedia.org/qubit

moneta rappresenta in questo istante entrambi gli stati. Solo attraverso l'osservazione di questa, aprendo gli occhi, possiamo essere in grado di determinare il risultato del lancio.

Questo aspetto di sovrapposizione è rappresentabile classicamente solo attraverso una simulazione probabilistica.

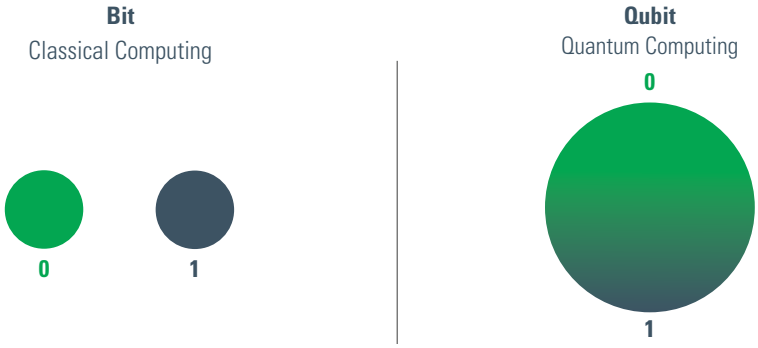

Figura 2: Immagine rappresentativa dello stato di superposizione.[9]

Entanglement: è il fenomeno per cui due particelle, inizialmente indipendenti, risultino "collegate" in modo che, benché distanti tra loro, la modifica dello stato di una di esse si rifletta anche sullo stato dell'altra. Questa caratteristica di un sistema è propria della meccanica quantistica e non è classicamente riproducibile.

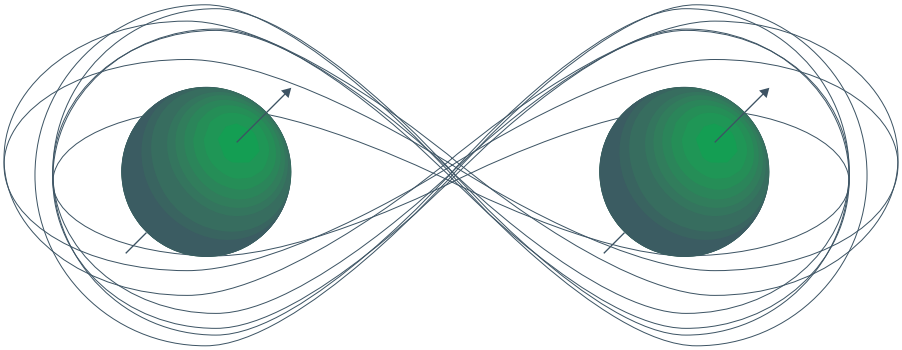

Figura 3: Stato di entanglement tra due qubit.[10]

È possibile intuire il concetto attraverso un altro esperimento mentale. Si prendano due biglie, una rossa e una blu. La colorazione è un loro tratto distintivo e completamente indipendente dalla colorazione reciproca. Si prendano ora due giare, non trasparenti, e si inserisca una biglia per giara ad occhi chiusi in modo da non sapere in quale è quella rossa e in quale quella blu. Una delle due giare, scelta casualmente, viene ora portata lontano, anche ai confini dell'universo conosciuto, mentre l'altra rimane nella stanza. L'informazione circa la colorazione di una biglia, che prima risultava del tutto indipendente, è ora invece intrinsecamente legata alla conoscenza della colorazione dell'altra biglia. Aprendo infatti la giara nella stanza e osservando che la biglia al suo interno è rossa, ad esempio, siamo in grado di determinare immediatamente che la biglia a chilometri di distanza da noi è blu.

Nelle prossime sezioni si analizzeranno diverse metodologie basate proprio sul principio di entanglement.

L'effetto tunnel quantistico: nel mondo microscopico, le particelle seguono regole diverse da quelle che sperimentiamo nella nostra vita quotidiana. Infatti, atomi ed elettroni possono attraversare barriere o ostacoli senza doverli superare fisicamente, come se avessero una capacità di "teletrasportarsi" dall'altro lato.

9 Immagine presa da https://qc-at-davis.github.io/QCC/How-Quantum-Computing-Works/The-Qubit/The-Qubit.html

10 Immagine presa da https://brilliant.org/wiki/quantum-entanglement/

Si immagini una montagna che blocca il passaggio di una particella. In un contesto classico, la particella dovrebbe scalare la montagna o trovare un modo per attraversarla, ma, a livello quantistico, la particella può attraversarla, apparentemente violando le leggi della fisica ordinaria come rappresentato in Figura 4.

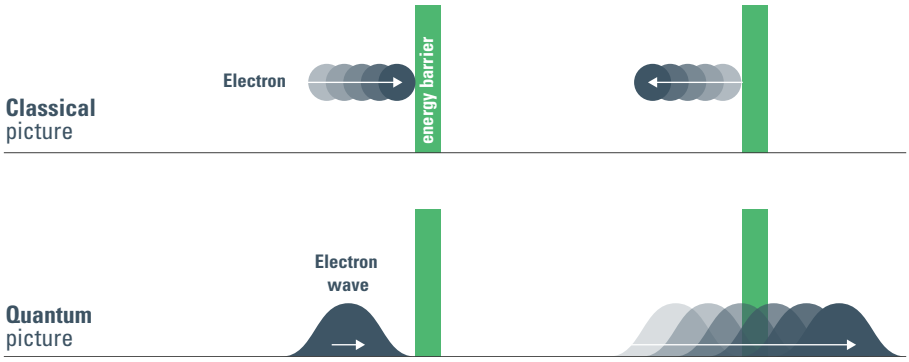

Figura 4: Esempio dell'effetto di tunnel quantistico in comparazione al comportamento nella meccanica classica.[11]

Esistono dispositivi quantistici che basano il loro funzionamento su questo principio. Ne sono un esempio il microscopio a effetto tunnel[12] e il computer a ricottura quantistica (Quantum Annealer) per la cui descrizione si rimanda alla sezione di dettaglio.

Il processo di misura: il processo di misura di un sistema quantistico digitalizza il valore rappresentato da un qubit rendendolo fruibile anche ad un elaboratore classico. Nella meccanica quantistica la misura rappresenta l'effettiva osservazione dell'informazione elaborata da un qubit. Prima della misura non è infatti possibile stabilire con certezza il risultato di un algoritmo quantistico, poiché il sistema può esistere simultaneamente in diverse possibili configurazioni in ragione della sovrapposizione degli stati descritta in precedenza. Tuttavia, dopo la misura, il sistema si stabilizza collassando in uno dei due stati classici.

Un'analogia utile per meglio comprendere il processo di misura è nuovamente rappresentata dal lancio di una moneta. Prima di osservare il risultato – testa o croce – la moneta è in uno stato sovrapposto, con entrambi i risultati possibili ciascuno con una certa probabilità. Non appena la si osserva, la moneta mostra un solo lato e il sistema collassa su un risultato specifico.

Ciò che rende la meccanica quantistica così intrigante è che fino a quando non viene effettuata una misura, il sistema quantistico può esistere in uno stato di sovrapposizione, permettendo a molteplici combinazioni di stati di coesistere. Solo attraverso la misura l'indeterminatezza quantistica si dissolve, ottenendo un risultato definito. È importante notare che l'operazione di misura comporta una perturbazione del sistema quantistico stesso. Di fatto, la misura rappresenta la conclusione delle operazioni di un algoritmo quantistico, come rappresentato in Figura 5.

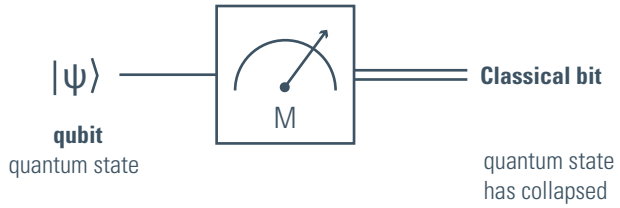

Figura 5: Processo di misurazione rappresentato in un circuito quantistico.[13]

Pertanto, se viene effettuata una seconda misura, a causa del precedente collasso dello stato quantistico determinato dalla prima, si otterrà sempre il medesimo output.

11 Immagine da https://ivypanda.com/essays/principle-of-work-quantum-tunneling-effect/

12 G. Binnig, H. Rohrer, Scanning tunneling microscopy, in IBM Journal of Research and Development, vol. 30, 1986.

13 Immagine presa da https://towardsdatascience.com/understanding-basics-of-measurements-in-quantum-computation-4c885879eba0

PRINCIPALI APPROCCI TECNOLOGICI

Gli algoritmi quantistici sviluppati a livello teorico presuppongono l'utilizzo di una macchina quantistica ideale, cioè che si comporti esattamente come descritto dai postulati della meccanica quantistica.

Tuttavia, i sistemi reali introducono degli errori che sono di diverso tipo e dipendono dalla tecnologia utilizzata. Essi possono essere tali da corrompere significativamente la computazione. Questi si possono mitigare o correggere essenzialmente introducendo ridondanza nelle risorse per il calcolo.

Le attuali famiglie di quantum computer esistenti in commercio sono denominate NISQ[14], acronimo di Near-term Intermediate Scale Quantum (devices). L'acronimo identifica delle macchine limitate nel numero di qubit (nel range 5-500) con un errore non trascurabile nelle fasi di calcolo. Oltre alla limitazione sul numero di qubit, sussiste un'ulteriore significativa limitazione sul numero di gate (ovvero sugli operatori algebrici applicati ai qubit) che è possibile applicare in sequenza. Esistono anche altri tipi di errori, ma vengono considerati di minor importanza, come, ad esempio, l'errore sulla misura.

Questa classe di dispositivi si contrappone alle macchine fault tolerant, le quali vedono oggi una significativa fase di sviluppo e che, quando realizzate, permetteranno di avere errori trascurabili al pari degli elaboratori classici odierni.

Ci si aspetta che tali computer quantistici "a prova di errore" possano essere creati migliorando la tecnologia attuale fino a raggiungere un livello di prestazioni tali da poter introdurre codici di correzione degli errori[15]. Fondamentale citare il fatto che queste tecnologie necessitano di un numero di qubit molto alto, in quanto l'informazione di un singolo qubit logico viene condivisa da più qubit fisici, introducendo ridondanza. Sebbene i computer NISQ attualmente disponibili non presentino al momento abbastanza risorse per implementare codici di correzione di errore, esistono comunque tecniche di error mitigation[16] per diminuire l'entità dell'errore, ottenendo un consumo di risorse modesto.

Esistono differenti approcci alla tecnologia hardware per lo sviluppo dei processori quantistici. Infatti, a differenza dei computer classici, che nella quasi totalità dei casi sono oggi basati su semiconduttori al silicio, nessuna tecnologia produttiva risulta al momento la migliore in assoluto per produrre computer quantistici.

Nel confrontare le tecnologie ci sono diversi aspetti di cui tener conto:

- il numero di qubit: maggior è il numero di qubit, più risorse è possibile processare e quindi cresce la dimensione dei problemi affrontabili;
- la temperatura di operatività: se l'approccio tecnologico con cui sono realizzati i qubit richiede un'operatività a temperature molto basse (15 millikelvin) la bontà del suo funzionamento è strettamente legato alla tecnologia di refrigerazione. Quest'ultima, oltre a incidere sul consumo energetico, rende complessa la miniaturizzazione di alcune componenti accessorie;
- la connettività dei qubit: se un qubit non può comunicare direttamente con un altro a causa dell'assenza della connessione fisica fra i due, occorre introdurre un ulteriore carico computazionale per spostare l'informazione quantistica a un terzo qubit adiacente al secondo con il quale si intende interfacciarsi;
- la fidelity dei gate a singolo e doppio qubit: rappresenta il grado di divergenza tra l'output di applicazione di un'operazione su un qubit (gate fisico) dal suo modello teorico matematico;
- i tempi T1 di decadimento e T2 di coerenza: T1 è il tempo in cui si ha almeno il 50% di probabilità che il qubit rimanga nello stato desiderato, mentre T2 è il tempo in cui il qubit può rimanere in sovrapposizione quantistica, prima di degenerare in uno stato classico, indipendentemente che esso sia o meno misurato.

In particolare, emergono due principali classi di hardware:

14 Preskill, John. "Quantum Computing in the NISQ era and beyond." Quantum 2 (2018): 79.

15 Raussendorf, Robert. "Key ideas in quantum error correction." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 370.1975 (2012): 4541-4565.

16 LaRose, Ryan, et al. "Mitiq: A software package for error mitigation on noisy quantum computers." Quantum 6 (2022): 774.

- **Quantum annealer**: tipo di hardware quantistico non universale, cioè pensato per approcciare e risolvere alcuni compiti specifici, quali i problemi di ottimizzazione. Ad oggi, la tecnologia a superconduttori è l'unica commercialmente utilizzata per implementare questo tipo di approccio;
- **Quantum computer a gate**: quantum computer che implementano un modello di operazioni algebriche sui qubit tramite operatori detti "gate". Questo approccio permette di implementare tutti gli algoritmi quantistici esistenti.

Nella tabella rappresentata sotto vengono riportati, in sintesi, quelle che sono le principali caratteristiche delle tecnologie più note in uso al momento.

Technology	Temperature of Operation	Number of Qubits	Speed of Gate	T1 Time	T2 Time
Superconducting Qubit	Millikelvin	Fino a migliaia	10^{-9} s	10^{-6} s	10^{-6} s
Trapped Ion	Millikelvin	Fino a centinaia	10^{-6}s	secondi	secondi
Photonics[17]	Temperatura ambiente	Fino a centinaia	10^{-12} s	10^{-9}s	10^{-9} s
Neutral Atoms[18]	Millikelvin	Fino a centinaia	10^{-6} s	10^{-3} s	10^{-3}s

STATO DEL MERCATO E DELLA RICERCA: VENDOR E PRODOTTI, CENTRI DI RICERCA ITALIANI E STARTUP

Il Quantum Computing e, più in generale, l'insieme di tecnologie ed approcci quantistici, compare ormai da anni all'interno dei principali radar e trend tecnologici configurandosi, nella maggior parte dei casi, come "tecnologia nascente" e lasciando più spazio ad elementi caratterizzati da un grado di maturità tecnologica e di mercato sensibilmente maggiore.

Ne risulta che l'esercizio sulla quantificazione del potenziale impatto (concordemente ritenuto rivoluzionario), lasci spazio al tentativo di prevedere il momento in cui possa verificarsi l'esplosione commerciale:

- secondo l'Hype Cycle Report di Gartner, il "tempo mancante" per l'informatica quantistica dovrebbe essere di 5-10 anni;
- IBM prevede che entro il 2028 ci saranno circa 1 milione di computer quantistici connessi nelle reti globali;
- Statista prevede un tasso di crescita annuale per le dimensioni del mercato globale dell'informatica quantistica compreso tra il 32% ed il 38% dal 2024.

Al netto delle previsioni, i dati fattuali continuano a testimoniare il crescente ed eterogeneo interesse nei confronti del mondo Quantum. Secondo il Quantum Technology Monitor di McKinsey, il totale degli investimenti in tecnologie quantistiche ha raggiunto un nuovo massimo nel 2023 (2,35 miliardi di dollari), anche se la crescita è stata solo dell'1% su base annua.

17 O'Brien, Jeremy. "Silicon Photonic Quantum Computing." APS March Meeting Abstracts. Vol. 2021. 2021.

18 Henriet, Loïc, et al. "Quantum Computing with neutral atoms." Quantum 4 (2020): 327.

Si riporta inoltre che:

- circa due terzi, ovvero il 68%, di tutti gli investimenti per l'avvio di QT dal 2001 si sono verificati nel 2021 e 2022;
- il 2022 è stato un anno di grandi affari: quattro su dieci dei più grandi accordi di investimento in tema QC sono stati chiusi nel 2022: SandboxAQ (500 milioni di dollari), Rigetti (345 milioni di dollari in un accordo SPAC), D-Wave (300 milioni di dollari in un accordo SPAC) e Origin Quantum (149 milioni);
- proseguono gli investimenti pubblici: gli Stati Uniti, l'Unione Europea e il Canada hanno investito rispettivamente 1,8 miliardi di dollari, 1,2 miliardi di dollari e 0,1 miliardi di dollari.

I settori su cui probabilmente ci sarà un maggior impatto economico dall'informatica quantistica nel breve periodo, oltre a quello dei servizi finanziari, sono l'automotive, il chimico-farmaceutico, e quello delle scienze biologiche, il cui valore potrebbe arrivare a 1,3 trilioni di dollari entro il 2035.

Tali investimenti provengono in larga parte dal settore privato, guidato dalle Big Tech statunitensi. Alla guida dei Paesi con il maggior numero di start-up si distinguono anche in questo caso gli Stati Uniti D'America, seguiti dal Canada. È utile sottolineare come, nonostante la generale tendenza negli investimenti in aziende e start-up si confermi robusta nei volumi, essa abbia subito un rallentamento nel 2022, come mostrato nella tabella seguente dove i dati vengono rappresentati tramite una suddivisione per settore di specializzazione degli investimenti. Probabilmente la ragione di ciò va ricercata congiuntamente nel fatto che tali investimenti seguono l'avvento di novità scientifiche (assolutamente rilevanti nel biennio 2020-21 per il mondo QT) e che questi sono generalmente allocati su piani pluriennali. In ultima analisi, va considerato anche l'aumento del costo del denaro che sappiamo essere tendenzialmente un fattore ostile agli investimenti su realtà innovative.

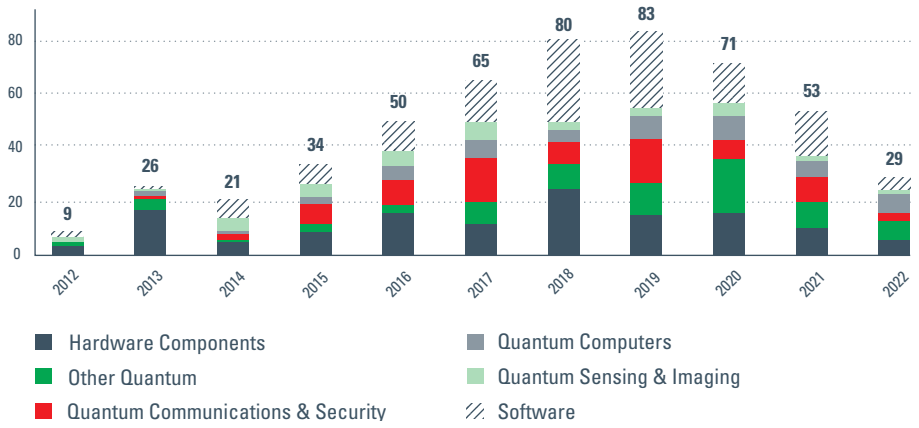

Figura 6: Creazione di nuove aziende legate al mondo del Quantum Computing.[19]

In generale, la parte più ingente degli investimenti relativi al Quantum Computing mira alla risoluzione delle problematiche legate all'hardware, ovvero a comprendere come costruire un elaboratore quantistico su cui implementare gli algoritmi teorici già formulati. Seppur in minor parte, ci si concentra anche nello sviluppo di sistemi di comunicazione basati sui principi della meccanica quantistica come pure sulla creazione di una nuova generazione di sensori largamente più sensibili dei classici sensori, come evidenziato nel seguente schema.

19 Fonte: https://www.canva.com/design/DAFVNCFvIvY/9xSCnlXlipEA4N8eUNBXDg/view

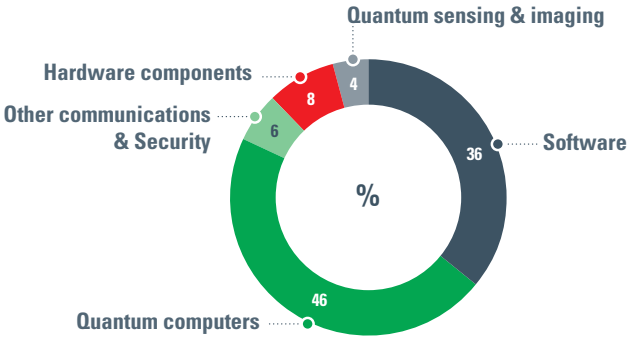

Figura 7: Investimenti nei diversi aspetti del Quantum Computing.[20]

Nel contesto europeo le aziende, gli enti e gli istituti finanziari stessi stanno cogliendo l'opportunità di sviluppo rappresentata proprio dal Quantum Computing. Tra queste troviamo nomi di grande rilievo[21] come le inglesi Barclays, per il Machine Learning[22], e HSBC, aderente al progetto europeo NEASQC[23], le francesi BNP Paribas, nel suo lavoro sulle simulazioni sull'andamento dei dati[24], e Crèdit Agricole, nelle sue applicazioni alle reti neurali[25], la stessa Banca d'Italia con la recente pubblicazione di "Quantum safe payment systems"[26]. Continuando l'analisi nel contesto dello scenario italiano, si pone come uno dei protagonisti la stessa Intesa Sanpaolo, attraverso lo sviluppo di diversi casi d'uso applicativi, gli investimenti della sua società di Venture Capital NEVA SGR, nonché la partnership col Politecnico di Torino per la creazione del Master in Quantum Communication and Computing. Tra i tanti enti di ricerca italiani impegnati nel settore del Quantum Computing, non ci si può esimere dal ricordare il Centro nazionale di Ricerca in HPC, Big Data e Quantum Computing, il Centro di Supercalcolo CINECA, l'Università Federico II di Napoli (che mira alla costruzione del primo quantum computer italiano) e il CNR-INO Quantum Communications Center.

Dal punto di vista dello sviluppo di questa tecnologia, il principale ambito di interesse risulta essere lo studio delle componenti che supportano la realizzazione di un quantum computer. Di seguito vengono elencati alcuni dei principali hardware vendor di computer quantistici e le tecnologie da loro utilizzate.

Tecnologia	Vendor
Quantum annealer a superconduttore	– D-Wave – Qilimangiaro
Quantum computer con gate a superconduttore	– IBM – Rigetti – Google
Quantum computer con gate a ioni intrappolati	– Quantinuum – IonQ
Quantum computer con gate a tecnologia fotonica	– Xanadu – PsiQuantum
Quantum computer con gate a atomi neutrali	– Pasqal

20 Fonte: https://thequantuminsider.com/reports/ - Quantum Technology Investment Update 2022 Review

21 https://thequantuminsider.com/2021/06/23/11-global-banks-probing-the-wonderful-world-of-quantum-technologies/

22 Emmanoulopoulos, D., & Dimoska, S. (2022). Quantum Machine Learning in Finance: Time Series Forecasting.

23 https://cordis.europa.eu/project/id/951821

24 Pracht, Rafał and Ryterski, Adam and Plewa, Julia and Stefaniak, Marek, FX Asian Option Pricing Using Quantum Computers (April 11, 2022). Available at SSRN: https://ssrn.com/abstract=4137397 or http://dx.doi.org/10.2139/ssrn.4137397

25 Patel, R., Hsing, C.-W., Sahin, S., Jahromi, S. S., Palmer, S., Sharma, S., Michel, C., Porte, V., Abid, M., Aubert, S., Castellani, P., Lee, C.-G., Mugel, S., & Orus, R. (2022). Quantum-Inspired Tensor Neural Networks for Partial Differential Equations.

26 https://www.bancaditalia.it/media/notizia/la-banca-d-italia-pubblica-oggi-quantum-safe-payment-systems/

Dal punto di vista del contributo scientifico, la Cina si aggiudica il primo posto seguita, a distanza ravvicinata, da Unione Europea e Stati Uniti d'America. La Cina d'altro canto sta fortemente puntando su questo campo anche grazie a fondi pubblici elargiti dal governo. Nello schema seguente[27] si presentano i primi dieci stati per numero di pubblicazioni scientifiche, ordinati però per l'impatto che hanno avuto sulla ricerca globale. Il grafico evidenzia come siano gli Stati Uniti d'America occupino anche in questo caso il primo posto in graduatoria.

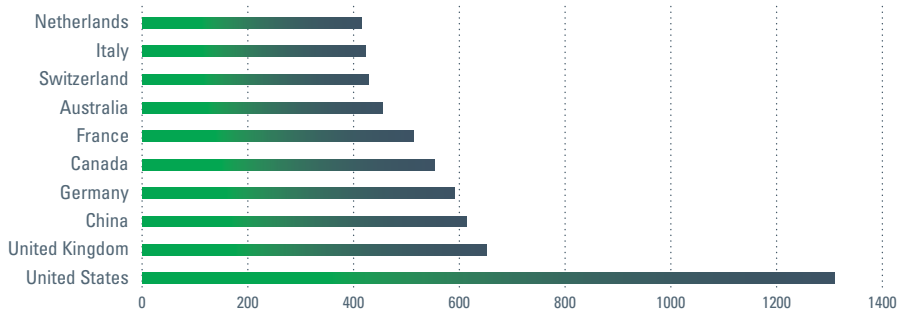

Figura 8: Top 10 countries nel mondo nel 2022 ordinate per h-index crescente.[28]

È inoltre interessante sottolineare come l'Unione Europea si ponga come leader nello scenario di nuove figure professionali legate ad ambiti di quantum technologies, seguita da India, Cina, Stati Uniti d'America.

Le figure di maggiore spicco hanno ricevuto una formazione avanzata su campi come matematica, statistica, fisica, chimica, elettronica ed ingegneria chimica, informatica e tecnologia delle comunicazioni. Tali settori si confermano dunque i più adatti nel delineare una figura professionale inerente al quantum, da quello che può essere un ruolo più tecnico-ingegneristico (Data Scientist, Software engineer, Software developer, Security Analyst) fino ad una posizione più manageriale (Project manager, Business development manager).

27 https://www.scimagojr.com Dati riguardanti il numero di articoli scientifici in ambito Computer Science con almeno h citazioni nell'anno 2022. In altri ambiti come matematica e fisica, gli Stati Uniti d'America confermano il primato

28 https://www.scimagojr.com Dati riguardanti il numero di articoli scientifici in ambito Computer Science con almeno h citazioni nell'anno 2022. In altri ambiti come matematica e fisica, gli Stati Uniti d'America confermano il primato

QUANTUM COMPUTING NEL MONDO FINANCE

Il Quantum Computing promette di superare le capacità computazionali e le performance in generale dei sistemi di calcolo classici, segnando di fatto l'inizio di una nuova era nell'informatica. Questo risulta di particolare interesse nel contesto finanziario, visto che i tipici casi d'uso sono caratterizzati da una elevata complessità computazionale oltre che da numerose e variegate variabili in input. Le implementazioni quantistiche dei corrispettivi metodi classici assicurerebbero non solo di andare a migliorare i tempi di calcolo attuali, ma pure di accrescere la qualità delle soluzioni, impiegando approcci unici basati su effetti quantistici quali superposition ed entaglement non replicabili nel contesto della computer science classica. Proprio per queste ragioni, i principali istituti bancari e assicurativi stanno investendo nell'utilizzo di algoritmi quantistici in diverse applicazioni. La cosiddetta Quantum Finance sembra dunque essere destinata a rivoluzionare il settore finanziario, non solo nell'approccio all'elaborazione dei dati, ma anche rivestendo un ruolo importante nella ricerca e nello sviluppo tecnologico degli strumenti finanziari e come attrattore di investimenti per il prossimo decennio.

Il focus di questa sezione è un confronto tra i principali approcci classici e le loro corrispondenti implementazioni quantistiche ad importanti problemi finanziari.

POTENZIALI APPLICAZIONI DEL QUANTUM COMPUTING NEL CAMPO FINANCE

Le applicazioni del Quantum Computing in ambito finanziario sono molteplici e possono integrarsi con la grande varietà di procedure classifiche già esistenti.

In particolare, le tecniche di calcolo quantistico in corso di sviluppo si concentrano essenzialmente nell'utilizzare questa capacità computazionale aggiuntiva per ottenere risultati più accurati e in minor tempo. Alcuni dei principali problemi affrontabili sono:

- Portfolio Optimization;
- Option Pricing;
- Credit Risk Analysis;
- Fraud Detection;
- Market Forecasting.

Portfolio Optimization

Il problema del portafoglio ottimo, consiste nell'identificazione del miglior portafoglio d'investimento (quindi della migliore combinazione di asset acquistabili sul mercato) per ottenere il maggior rendimento possibile contenendone al contempo il rischio.

Tramite l'integrazione di procedure relative al Quantum Computing negli schemi già esistenti, il processo di valutazione dei possibili portafogli potrebbe essere più veloce ed accurato, dato l'aumento delle possibilità computazionali a disposizione degli analisti.

Si pensi a come, per esempio, i tempi di esecuzioni garantiti da questi metodi permettano di svolgere una quantità di simulazioni di scenari finanziari significativamente più ampia, tale da assicurare una soluzione più precisa, resiliente ed accurata al cliente.

In generale, la risoluzione di problemi che consistono nel trovare il minimo o il massimo di una funzione, soddisfacendo diversi vincoli, è alla base della modellazione matematica di diversi problemi del mondo della finanza. La funzione da minimizzare (o massimizzare) prende il nome di funzione obiettivo e, allo stesso tempo, è comune la presenza di un insieme di vincoli che devono essere soddisfatti nel processo di ricerca della soluzione ottima. Questo tipo di problemi può essere formulato utilizzando variabili i cui valori possono essere di diverso tipo come interi, binari (ossia 0 e 1), o continui.

Il raggiungimento di risultati di questo tipo può essere complesso visto che il numero di possibili portafogli da valutare cresce molto velocemente con l'aumentare del numero e del tipo di azioni acquistabili. I vincoli inseribili in questo tipo di modellazione possono essere di diverso tipo. Ad esempio, si potrebbe richiedere che il portafoglio d'investimenti selezioni un numero equo di titoli appartenenti a settori industriali differenti.

Grazie alla sua flessibilità, questo tipo di modellazione permette di affrontare, oltre al già discusso problema di ottimizzazione di un portafoglio, anche i problemi di **swap netting**[29] e di **financial crashes**.[30][31][32]

Al fine di comprendere la potenziale complessità legata alla ricerca della soluzione ottimale, in Figura 9 è riportata la rappresentazione geometrica dell'output di un algoritmo che si occupa di ricercare il un punto di minimo (o massimo) di una determinata funzione obiettivo nel rispetto dei vincoli imposti.

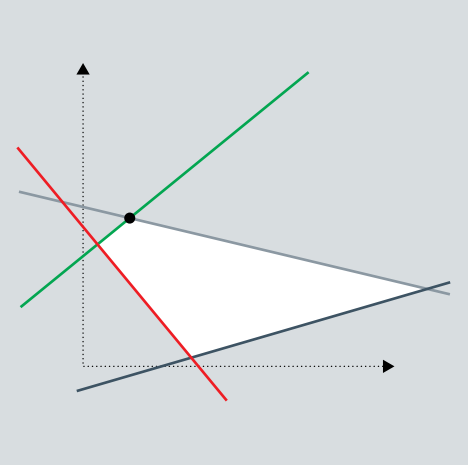

Figura 9: Grafico rappresentante la regione creata dai possibili valori delle variabili in un problema di programmazione lineare a variabili continue, in cui una regione è stata esclusa dai vincoli (regione blu) e quella restante risulta essere quella compatibile in cui cercare l'ottimo (regione bianca). Il punto di ottimo che soddisfa i vincoli e massimizza la funzione obiettivo è rappresentato, a titolo di esempio, dal punto nero.

Per molti problemi e scenari reali, specie in quelli in cui i vincoli devono tenere conto di numerose e complesse relazioni fra le variabili di interesse, si osserva un significativo aumento dello sforzo computazionale necessario alla massimizzazione o minimizzazione della funzione obiettivo.

Questo aspetto è di particolare rilevanza in applicazioni quali Portfolio Optimization ed Hedging, dove è importante tener contro delle diverse correlazioni e vincoli tra le variabili di interesse[33]. Allo stesso modo, la formulazione tradizionale del problema di ottimizzazione del portafoglio, che risale a Markowitz[34] e rappresenta un caposaldo di questa teoria, diminuisce la sua efficienza computazionale al crescere di queste dimensioni.

In questo contesto, la tecnologia sviluppata attraverso i Quantum Annealer, il cui principale vendor è D-Wave, sembrerebbe risultare al momento quella di maggior efficacia per indirizzare il problema. La formulazione **Quadratic Unconstrained Binary Optimization (QUBO)**, che impiega solamente variabili binarie, permette di gestire agevolmente la presenza di vincoli anche non lineari tra i dati in input al problema. Per applicare questo metodo risolutivo su un Quantum Annealer disponibile oggi ci si affida a solver di ottimizzazione che suddividono il problema in sotto-problemi di dimensione ridotta, trovando poi la migliore soluzione globale.

29 G. Rosenberg, C. Adolphs, A. Milne, and A. Lee. Swap netting using a quantum annealer. White Paper 1Qbit, 2016.

30 Matthew Elliott, Benjamin Golub, and Matthew O. Jackson. Financial networks and contagion. American Economic Review, 104(10):3115–53, October 2014.

31 Román Orús, Samuel Mugel, and Enrique Lizaso. Forecasting financial crashes with Quantum Computing. Phys. Rev. A, 99(6), Jun 2019.

32 Michael Fellner, Kilian Ender, Roeland ter Hoeven, and Wolfgang Lechner. Parity quantum optimization: Benchmarks. arXiv preprint arXiv:2105.06240, 2021.

33 Mattesi, M., Asproni, L., Mattia, C., Tufano, S., Ranieri, G., Caputo, D., & Corbelletto, D. (2023). Financial Portfolio Optimization: a QUBO Formulation for Sharpe Ratio Maximization.

34 Marling, Hannes, and Sara Emanuelsson. "The Markowitz portfolio theory." November 25 (2012): 2012.

Il **Quantum Annealing** è un algoritmo euristico che sfrutta il tunneling quantistico proprio per ottenere soluzioni migliori ad un problema di ottimizzazione[35]. Dal punto di vista applicativo, l'algoritmo inizia identificando una prima soluzione al problema, in una versione estremamente semplificata, ed evolve nel tempo avvicinandosi a poco a poco alla soluzione ottimale. Se questa evoluzione è sufficientemente lenta, grazie al principio adiabatico, il sistema si porta allo stato di equilibrio corrispondente alla soluzione ottimale del problema iniziale. In Figura 10 viene rappresentato come il Quantum Annealing permette di sfruttare il Quantum Tunneling[36]. Il sistema passa da uno stato ad un altro seguendo la traiettoria identificata dalla linea rossa, riducendo il numero di step computazionali rispetto a quelli necessari per effettuare lo stesso cambio di stato in una generale procedura classica (linea blu).

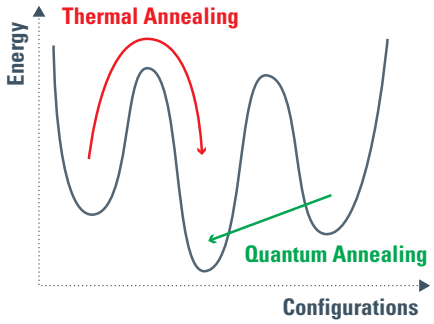

Figura 10: Quantum annealing comparato con la procedura di annealing legata alla termodinamica.[37]

Il Quantum Annealing è una procedura che può anche essere parzialmente replicata su computer classici in alternativa al simulated annealing[38]; lo svantaggio in questo caso è che la simulazione non approssimata di un sistema quantistico ha un costo, in termini di risorse computazionali, che cresce esponenzialmente rispetto alla dimensione del sistema e questo la rende di difficile applicazione su problemi reali.

Un'altra possibile alternativa alla risoluzione dei problemi di ottimizzazione è rappresentata delle cosiddette metodologie **Quantum-Inspired**. Questi approcci nascono con l'obiettivo di scrivere algoritmi classici più efficienti, prendendo ispirazione dalle controparti quantistiche, ma adattandoli ad essere eseguiti su infrastruttura di calcolo tradizionali ultra-performanti o HPC (High Performance Computing), rendendo possibile il conseguimento di un potenziale vantaggio già nel breve termine.

In particolare, le capacità di parallelizzazione massiva delle attuali Graphics Processing Units (GPUs) permettono di risolvere problemi QUBO (Quadratic Unconstrained Binary Optimization) di larga scala, superando così le limitazioni legate alle dimensioni poste dagli attuali quantum device[39].

Le potenzialità di questo tipo di approcci risultano già evidenti in relazione a diversi problemi di ottimizzazione, proprio per la loro capacità di interpretare in modo efficace le correlazioni tra i dati[40] e di trovare quindi soluzioni ottimali al problema posto.

35 Apolloni, Bruno, Nicolò Cesa-Bianchi, and Diego De Falco. "A numerical implementation of "quantum annealing"." Stochastic Processes, Physics and Geometry: Proceedings of the Ascona-Locarno Conference. 1990.

36 Liu, Yizhou, Weijie J. Su, and Tongyang Li. "On Quantum Speedups for Nonconvex Optimization via Quantum Tunneling Walks." Quantum 7 (2023): 1030.

37 Immagine estratta da: https://steemit.com/science/@gotgame/quantum-annealing

38 Kirkpatrick, Scott, C. Daniel Gelatt Jr, and Mario P. Vecchi. "Optimization by simulated annealing." science 220.4598 (1983): 671-680.

39 Tiunov, E. S., Ulanov, A. E., & Lvovsky, A. I. (2019). Annealing by simulating the coherent Ising machine. Optics Express, 27(7), 10288. https://doi.org/10.1364/oe.27.010288

40 Bozhedarov, A. A., Boev, A. S., Usmanov, S. R., Salahov, G. V., Kiktenko, E. O., & Fedorov, A. K. (2023). Quantum and quantum-inspired optimization for solving the minimum bin packing problem.

Option Pricing e Quantum Monte Carlo Integration (QMCI)

Altra promettente applicazione della computazione quantistica in ambito finanziario riguarda il pricing degli strumenti derivati, in particolare delle opzioni; come evidenziato dal lavoro svolto congiuntamente da JPMorgan, ETH Zurich ed IBM Quantum riguardante le American Option, le Asian Option, le European Option e le Bermudan Option[41].

Generalmente, per la valutazione del prezzo delle opzioni in un determinato istante di tempo gli analisti operano delle simulazioni (tramite metodi Monte Carlo), che si rivelano spesso onerose in termini di tempo, specialmente per modelli complessi e di larga dimensione. Nello scenario più semplice, il valore delle opzioni dipende solo da un singolo instante temporale nel futuro, mentre in uno scenario più realistico il valore è legato all'evoluzione delle risorse fino ad una data prestabilita nel futuro.

Specialmente in questi ultimi casi, il Quantum Computing ha il potenziale di migliorare significativamente l'efficienza delle simulazioni Monte Carlo ed ottenere dei risultati più precisi in un tempo inferiore.

La metodologia usata nel determinare il prezzo delle opzioni su un quantum computer universale è la Quantum Amplitude Estimation (QAE)[42], un algoritmo che garantisce un'accelerazione quadratica nel calcolo se comparato al metodo Monte Carlo suo corrispettivo classico. QAE è una procedura che può essere usata per stimare il valore atteso di una data funzione ed è basato su l'algoritmo di Amplitude Amplification[43], impiegato anche nella procedura di Grover[44]. Si tratta quindi di uno strumento con grande potenzialità nel pricing di opzioni (e – più in generale – di strumenti derivati), giacché permette di stimare più rapidamente, con meno dati in input e con maggior precisione il ricavo previsto dagli stessi. In particolare, l'implementazione di QAE per l'option pricing nella finanza prevede che:

- i dati in input siano codificati in stati quantistici tramite qubit;
- una serie di operazioni (quantum gates) sia applicata in modo da "imitare" l'evoluzione temporale dell'opzione finanziaria e codificare il ricavo atteso in uno stato quantistico;
- si effettui una misura dello stato quantistico del qubit deputato a contenere il valore stimato per il ricavo dell'opzione cercato.

Se confrontato con le implementazioni classiche dei metodi Monte Carlo, il vantaggio chiave di QAE è rappresentato sia dall'efficienza computazionale, sia dalla capacità di gestire simultaneamente molteplici scenari. Tuttavia, l'implementazione di QAE richiede un elevato numero di qubit e uno sviluppo avanzato degli hardware quantistici per renderli sufficientemente coerenti per il tempo necessario all'esecuzione dell'algoritmo. Nonostante ciò, le tecniche di correzione dell'errore stanno migliorando sempre più la sua utilizzabilità su problemi più complessi e di dimensioni crescenti.

Generalmente una simulazione Monte Carlo consta di tre diverse fasi:

- **identificazione della distribuzione dei dati di input**: è possibile identificare ogni distribuzione di probabilità, continua o discreta, utilizzando un insieme di parametri. Nel raggiungere questo obiettivo ci sia affida spesso al metodo di verosimiglianza[45];
- **generazione delle variabili casuali**: una volta aver individuato la distribuzione di probabilità che governa i dati, è necessario andare a estrarre dei valori casuali dalla stessa distribuzione. Per fare questo si ricorre alla funzione inversa della funzione di densità di probabilità o al metodo Bootstrap, come rappresentato in Figura 11;

41 Nikitas Stamatopoulos, Daniel J. Egger, Yue Sun, Christa Zoufal, Raban Iten, Ning Shen, and Stefan Woerner. Option pricing using quantum computers. Quantum, 4:291, Jul 2020

42 Brassard, Gilles, et al. "Quantum amplitude amplification and estimation." Contemporary Mathematics 305 (2002): 53-74.

43 Brassard, Gilles, et al. "Quantum amplitude amplification and estimation." Contemporary Mathematics 305 (2002): 53-74.

44 Grover, Lov K. "Quantum computers can search arbitrarily large databases by a single query." Physical review letters 79.23 (1997): 4709.

45 Haynes, W. (2013). Maximum Likelihood Estimation. In: Dubitzky, W., Wolkenhauer, O., Cho, KH., Yokota, H. (eds) Encyclopedia of Systems Biology. Springer, New York, NY. https://doi.org/10.1007/978-1-4419-9863-7_1235

Figura 11: Distribuzione di densità di probabilità ottenuta tramite campionamento Bootstrap.[46]

- **analisi e decisione finale**: si valutano statisticamente i dati generati dal modello Monte Carlo con l'obiettivo di trovare la miglior soluzione al problema.

Nella sua implementazione classica, il metodo Monte Carlo stima il valore atteso di una risorsa che dipende da un certo numero di variabili casuali. Per fare questo, in accordo con la disuguaglianza di Chebyshev e la legge dei grandi numeri[47], la stima dell'errore che commettiamo nella stima decresce con il numero di campionamenti.

Nella sua implementazione quantistica, QMCI è in grado di sfruttare il vantaggio quantistico dato dalla procedura di Quantum Amplitude Estimation[48], per ottenere un vantaggio quadratico nella stima dell'errore. Un risultato importante da sottolineare è che in questo contesto è possibile ottenere un'approssimazione ad un errore desiderato e tramite un numero di operazioni nell'ordine di (e^{-1}). In Figura 12 si mostra una comparazione di diversi promettenti approcci di simulazioni Monte Carlo[49]. In modo particolare, sull'asse delle ascisse si ha il numero di ripetizioni del circuito trasformazione dei dati iniziali, mentre sull'asse delle ordinate si trova una misura basata sull'errore quadratico medio. È possibile dunque notare che ad una maggiore complessità nella codifica degli stati quantistici, corrisponde in generale una maggiore qualità della soluzione.

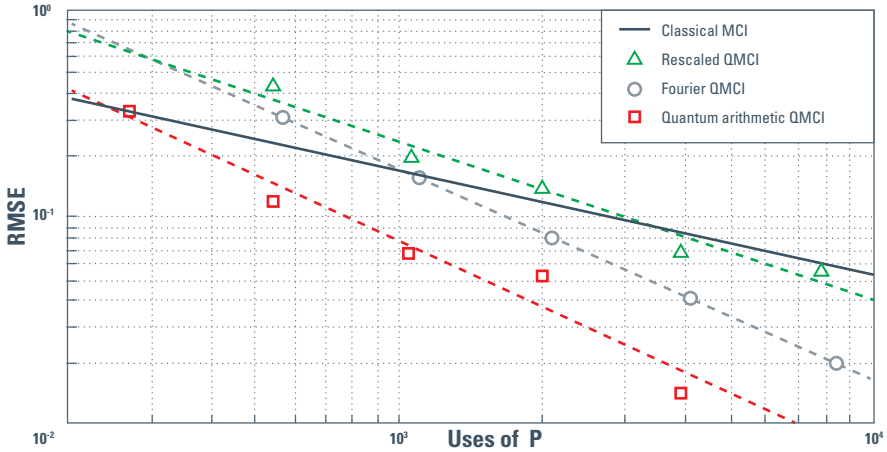

Figura 12: Comparazione di diverse procedure di simulazione Monte Carlo sulla stessa distribuzione di dati.

46 Immagine presa da https://towardsdatascience.com/introduction-to-bootstrapping-in-data-science-part-2-ef7236e464a7.

47 Christian P Robert, George Casella, and George Casella. Monte Carlo statistical methods, volume 2. Springer, 2004.

48 Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. Quantum Computation and Information, page 53–74, 2002.

49 Herbert, Steven. (2022). Quantum Monte Carlo Integration: The Full Advantage in Minimal Circuit Depth. Quantum. 6. 823. 10.22331/q-2022-09-29-823.

Alcune delle metodologie analizzate dalla Figura 12 sono varianti del metodo originale che però non vengono qui approfondite viste l'applicazione ancora marginale[50].

Nell'approccio classico si fa spesso riferimento al modello Black-Scholes[51], secondo il quale il prezzo delle risorse analizzate evolve assumendo che la volatilità si mantenga costante. Le equazioni che descrivono questo modello governano l'andamento del prezzo di una semplice European Option. Tuttavia, quando si trattano opzioni più complesse, si preferisce esplorare soluzioni ottenute con approcci basati su simulazione Monte Carlo, piuttosto che risolvere il corrispettivo sistema di equazioni analitico; ciò può richiedere in certi casi un notevole sforzo sia a livello software che hardware. Si è visto come, in tal senso, l'integrazione quantistica del metodo Monte Carlo (QMCI) possa comportare un vantaggio rispetto a quella classica. Infatti, l'applicazione della variante quantistica delle simulazioni Monte Carlo è in grado di considerare e analizzare le relazioni di correlazione tra i dati della serie storica anche in scenari in cui il payoff, ossia il rendimento dell'opzione, è dipendente dalle relazioni fra le variabili in gioco nei diversi momenti temporali considerati.

Diverse implementazioni di QMCI possono essere, infatti, impiegate per opzioni a percorso dipendente, cioè correlate a diversi attimi temporali, come le Asian option[52] o alle opzioni multi-risorsa[53]. Un'altra applicazione della metodologia QMCI riguarda le American option, attraverso gli stopping times. Un tempo di fine ottimale[54] è il momento che consente all'investitore un payoff maggiore, o uguale, a quello che potrebbe ricavare continuando nel tempo. Questo tipo di approccio è permesso dalla natura delle American options stesse, dal momento che queste possono essere esercitate, comprate o vendute, in un qualsiasi istante temporale, diversamente da quelle europee o asiatiche che devono attendere un tempo di maturità. Questo tempo ottimale può essere calcolato utilizzando la versione quantistica del metodo Monte Carlo (QMCI), utilizzando campionamenti di payoff che sono stati esercitati in tempi ottimali[55]. Infine, un approccio simile risulta applicabile anche alle Bermudan option, che sono vincolate ad essere esercitate in determinati istanti temporali[56].

Credit Risk Analysis

L'analisi del rischio di credito consiste nel valutare la probabilità di insolvenza di un prestito o un mutuo, prendendo in considerazione vari fattori quali, per esempio, la storia creditizia del debitore, le sue condizioni finanziarie, la sua capacità di rimborso e il profilo di rischio complessivo.

Anche in questo caso, il processo decisionale per l'approvazione di un prestito viene supportato dalla simulazione di un'elevata quantità di scenari tramite l'utilizzo di metodi Monte Carlo.

L'integrazione della componente quantistica, oltre alla diminuzione delle tempistiche, permetterebbe all'analista di considerare nelle proprie valutazioni un maggior numero di "eventi rari" con efficacia, assicurando un miglior contenimento del rischio all'istituto finanziario creditore.

Un esempio di caso d'uso è la stima dell'Economic Capital Requirement (ECR), ovvero la differenza tra il Value at Risk (VaR) [57] [58] e il valore atteso di una data distribuzione di perdita. L'ECR è un'importante metrica di rischio perché riassume la quantità di capitale richiesta per rimanere solvibile fissato un certo livello di confidenza. Le metriche di rischio come VaR ed ECR sono spesso calcolate per molti scenari diversi. In ambito classico, le simulazioni Monte Carlo (MC) sono il metodo preferenziale utilizzato per generare questi scenari. La valutazione del rischio di credito è un problema di simulazione di eventi rari che richiede molti campioni, rendendolo quindi costoso da un punto di vista computazionale. Il medesimo problema può essere affrontato con computer quantistici basati con il già citato algoritmo di Quantum Amplitude Estima-

50 Herbert, Steven. (2022). Quantum Monte Carlo Integration: The Full Advantage in Minimal Circuit Depth. Quantum. 6. 823. 10.22331/q-2022-09-29-823.

51 Fischer Black and Myron Scholes. The pricing of options and corporate liabilities. In World Scientific Reference on Contingent Claims Analysis in Corporate Finance: Volume 1: Foundations of CCA and Equity Valuation, pages 3–21. World Scientific, 2019.

52 Patrick Rebentrost, Brajesh Gupt, and Thomas R. Bromley. Quantum computational finance: Monte Carlo pricing of financial derivatives. Physical Review A, 98(2), Aug 2018

53 Nikitas Stamatopoulos, Daniel J. Egger, Yue Sun, Christa Zoufal, Raban Iten, Ning Shen, and Stefan Woerner. Option pricing using quantum computers. Quantum, 4:291, Jul 2020

54 Albert N Shiryaev. Optimal stopping rules, volume 8. Springer Science & Business Media, 2007.

55 João F. Doriguello, Alessandro Luongo, Jinge Bao, Patrick Rebentrost, and Miklos Santha. Quantum algorithm for stochastic optimal stopping problems with applications in finance, 2021.

56 Koichi Miyamoto. Bermudan option pricing by quantum amplitude estimation and chebyshev interpolation, 2021.

57 Stefan Woerner and Daniel J. Egger. Quantum risk analysis. npj Quantum Information, 5(1), Feb 2019.

58 D. J. Egger, R. Garcia Gutierrez, J. Mestre, and S.Woerner. Credit risk analysis using quantum computers. IEEE Transactions on Computers, 70(12):2136–2145, Dec 2021.

tion (QAE), il cui vantaggio chiave è quello di poter fornire un'accelerazione quadratica alla simulazione. In Figura 13, è possibile osservare il confronto tra una procedura classica e una basata su QAE[59].

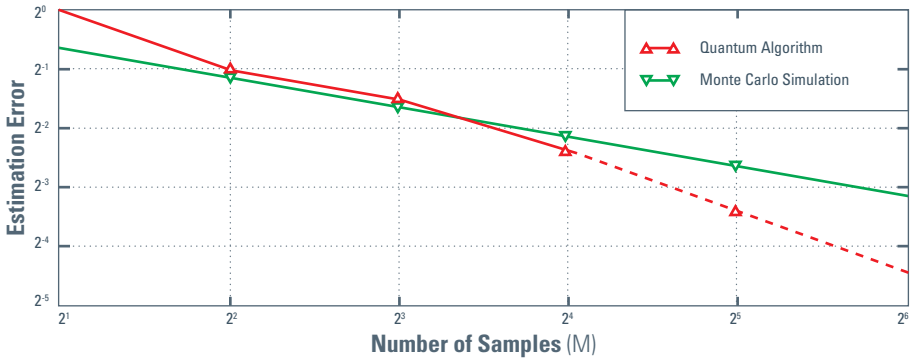

Figura 13: Comparazione dei risultati per l'analisi del rischio ottenuti da metodo classico e quantum.[60]

Si noti come, nonostante la maggior precisione del metodo classico quando il numero di campioni considerato è limitato, l'algoritmo quantistico ottiene progressivamente un vantaggio considerevole in accuratezza con l'aumentare del numero degli scenari.

Modellazione e stima del rischio ricoprono aspetti fondamentali nelle applicazioni finanziarie, motivando di conseguenza una crescente attenzione verso gli approcci di Quantum Computing in grado di portare benefici significativi. In letteratura si assiste a un crescente interesse verso lo studio di algoritmi che meglio catturino le diverse complessità degli scenari reali, come nelle strategie di Credit Risk Analysis[61].

Fraud Detection

Banche ed assicurazioni, così come molteplici compagnie in settori al di fuori dei servizi finanziari, hanno la necessità di implementare sistemi atti a verificare la veridicità o l'idoneità delle operazioni inerenti ai propri servizi, dalle transazioni bancarie alle richieste di risarcimento assicurativo.

L'obiettivo è quello di identificare frodi o anomalie all'interno dei flussi di dati, in modo da mantenere un elevato grado di sicurezza, evitare tentativi di riciclaggio di denaro e prevenire potenziali perdite derivanti da risarcimenti richiesti per falsi sinistri.

La Fraud Detection è uno degli ambiti principali in cui si evidenzia una crescente attenzione al Quantum Computing, per indirizzare i seguenti aspetti critici del problema:

- a livello operativo, un sistema antifrode necessita di una grande potenza di calcolo per valutare velocemente se una transazione sia o meno lecita e, in caso non lo sia, disporre una sua eventuale interruzione (a priori) o storno (a posteriori);
- a livello strategico, un inadeguato sistema antifrode, potrebbe comportare un degrado della qualità del servizio o addirittura un danno reputazionale per l'istituto finanziario.

Una possibile strategia per individuare le anomalie consiste nell'impiegare algoritmi di Machine Learning. Tuttavia, ciò non si rivela banale all'atto pratico[62], poiché i dati in input sono in genere fortemente sbilanciati: il numero di record anomali è – quasi sempre – una percentuale molto esigua del totale delle transazioni. Per questo motivi classificatori supervised, che suddividono i record sulla base di etichette assegnate ai dati di training, si rivelano poco efficaci a meno di non effettuare un pesante pre-processing degli stessi, sotto-campionando

59 Stefan Woerner and Daniel J. Egger. Quantum risk analysis. npj Quantum Information, 5(1), Feb 2019.

60 Immagine da Stefan Woerner and Daniel J. Egger. Quantum risk analysis. npj Quantum Information, 5(1), Feb 2019.

61 Dri E, Aita A, Giusto E, Ricossa D, Corbelletto D, Montrucchio B, Ugoccioni R. A More General Quantum Credit Risk Analysis Framework. Entropy. 2023; 25(4):593. https://doi.org/10.3390/e25040593

62 Raj, S. Benson Edwin, and A. Annie Portia. "Analysis on credit card fraud detection methods." 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET). IEEE, 2011.

i record legittimi (quindi escludendo una parte delle informazioni utili all'addestramento) o sovra-campionando quelli anomali (ad esempio generandone di nuovi attraverso tecniche di data synthesis o data mimicking). Il Quantum Computing propone nuovi paradigmi che mirano a superare queste difficoltà. Tra gli approcci più comuni in questo ambito spiccano quelli ibridi, ovvero tecniche che utilizzano sia risorse classiche sia quantistiche. Un esempio sono le reti neurali ibride: la parte più onerosa del calcolo, legata alla trasformazione dei dati finalizzata a scoprire schemi che permettano di identificare le frodi, viene delegato all'hardware quantistico, mentre l'ottimizzazione dei parametri della rete rimane in carico all'hardware classico.

In particolare, recenti studi hanno dimostrato come l'impiego di un tipo specifico di reti neurali, le Generative Adversarial Networks (GANs), sia utile a ribilanciare la distribuzione dei dati di transazioni corrette e fraudolente, permettendo così di allenare il classificatore con maggior precisione. Una possibile implementazione [63] fa riferimento alla progettazione di GAN tramite un modello generativo ibrido classico-quantum, allenato grazie ad un algoritmo variazionale, e un modello discriminativo classico. L'unione di layer classici e di circuiti quantistici parametrici (Variational Quantum Classifiers – VQC) è la scelta preferibile, nonché l'unica applicabile su problemi reali allo stato dell'attuale sviluppo dell'hardware quantistico. In Figura 14, si presenta un modello di rete neurale ibrido, in cui la parte di classificazione ha implementazione quantistica.

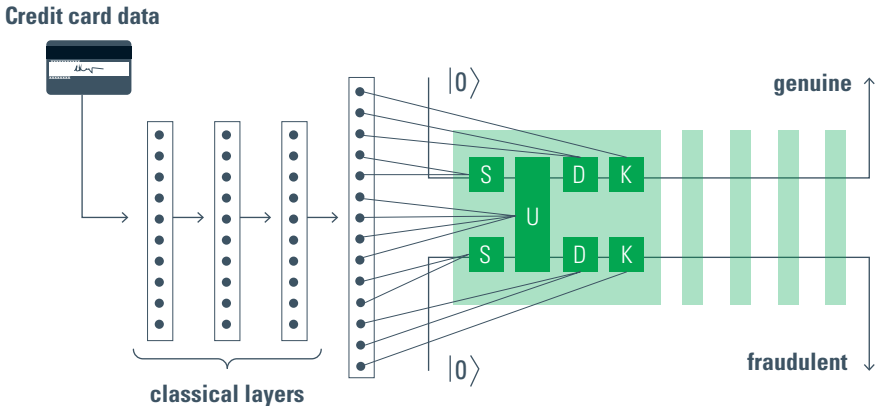

Figura 14: Identificazione di anomalie applicata su una carta di credito dove la parte classica controlla i parametri di input per la parte quantistica.[64]

Sono stati inoltre sviluppati metodi che sfruttano approcci full-quantum come Quantum Amplitude Estimation (QAE) per dare uno speedup ad alcune classi di algoritmi basati sulla stima a densità[65].

Infine, nel contesto dei problemi di categorizzazione, esistono anche implementazioni unsupervised basate sui **Quantum Kernels**[66]. Infatti, diversi algoritmi di questo tipo come la Principal Component Analysis (PCA) partono mappando i dati originali in un nuovo set di dati contenente nuove feature (ovvero le variabili di partenza per la classificazione), un esempio è dato in Figura 15.

Grazie a queste nuove feature, ottenute mediante clustering, è possibile categorizzare meglio i dati migliorando al contempo le performance[67].

63 Herr, D., Obert, B., & Rosenkranz, M. (2021). Anomaly detection with variational quantum generative adversarial networks.

64 Immagine presa da Killoran, N., Bromley, T. R., Arrazola, J. M., Schuld, M., Quesada, N. s, & Lloyd, S. (2019) Continuous-variable quantum neural networks. Physical Review Research, 1(3). https://doi.org/10.1103/physrevresearch.1.033063

65 Ming-Chao Guo, Hai-Ling Liu, Yong-Mei Li, Wen-Min Li, Su-Juan Qin, Qiao-Yan Wen, and Fei Gao. Quantum algorithms for anomaly detection using amplitude estimation. arXiv preprint arXiv:2109.13820, 2021.

66 Dongkuan Xu and Yingjie Tian. A comprehensive survey of clustering algorithms. Annals of Data Science, 2(2):165–193, 2015.

67 Di Marcantonio, F., Incudini, M., Tezza, D. et al. Quantum Advantage Seeker with Kernels (QuASK): a software framework to speed up the research in quantum machine learning. Quantum Mach. Intell. 5, 20 (2023). https://doi.org/10.1007/s42484-023-00107-2

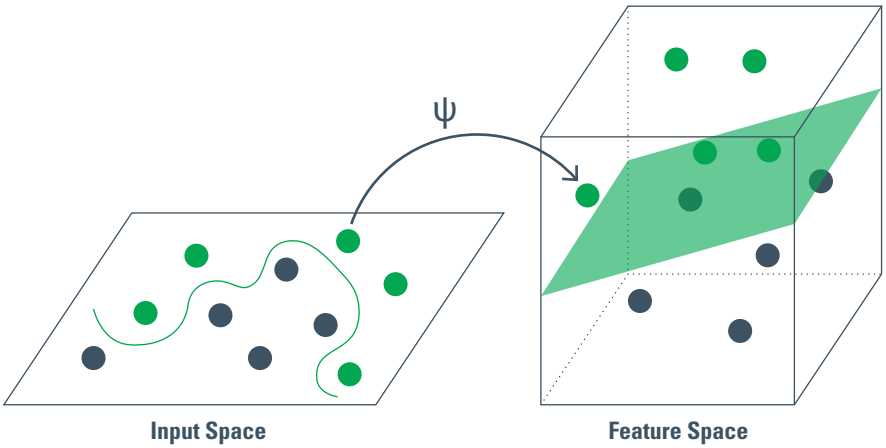

Figura 15: Esempio di traformazione di dati classici in informazione quantistica attraverso una feature map.[68]

Il punto di forza di questa metodologia risiede nella possiblità di considerare solo quelle feature veramente di interesse, senza dunque aver necessità di esplicitarle tutte e tenerne davvero conto per effettuare la categorizzazione.

Market Forecasting:
La previsione di serie storiche, come ad esempio il valore di titoli di borsa, rappresenta una componente decisiva nella scelta delle strategie di investimento. Appare chiaro come questa previsione possa condurre l'investitore verso una scelta piuttosto che ad un'altra.

I dati sotto forma di serie temporali sono tra i più diffusi in ambito finanziario. Le principali tecniche di trend analysis oggi utilizzate si basano su componenti statistiche in grado di dare forma all'evoluzione nel tempo dei dati, anche tenendo conto dell'influenza di altre serie storiche ad essi collegate: i processi stocastici[69]. Questi modelli, parametrici e non, sono in grado di andare a descrivere una serie storica tramite analisi concentrate sull'autocorrelazione dei dati, la loro stagionalità, la loro tendenza di lungo periodo e sull'influenza di fattori esterni. Lavorando tramite questa metodologia risulta inoltre necessario filtrare solo i dati di interesse e gestire la presenza di dati mancanti o dati che influiscono in modo da rendere fuorvianti i risultati statistici.

Essendo un dispositivo in grado di lavorare in modo probabilistico, un quantum computer si rivela particolarmente adatto a valutare la grandezza sottesa ad un processo stocastico. In alternativa, per la previsione di serie storiche è possibile impiegare il deep learning: le reti neurali sono infatti in grado di intercettare caratteristiche dei dati in modo più dinamico al variare del tempo, facendo particolare leva sulla loro ricorsività. Tuttavia, un tale approccio richiede la valutazione del bilanciamento tra numero di dati necessari e le risorse computazionali atte ad elaborarli.

68 Immagine da https://www.turing.com/kb/designing-of-different-kernels-in-machine-learning-deep-learning

69 Brockwell PJ and Davis RA (2002), Introduction to Time Series and Forecasting, (Second Edition), Springer

SINTESI DEI RISULTATI DERIVANTI DALL'APPROCCIO QUANTISTICO

Nella sezione precedente si sono confrontate le principali tecniche classiche per la risoluzione dei problemi finanziari più onerosi da un punto di vista computazionale e alcune delle loro controparti quantistiche.

Da quanto analizzato, è possibile intravedere un generale aumento delle prestazioni, sia riguardo le tempistiche di esecuzione, sia in relazione all'accuratezza delle soluzioni, per la risoluzione di differenti problemi che risultano di grande interesse per il mondo dei servizi finanziari, dalla Portfolio Optimization alla Fraud Detection.

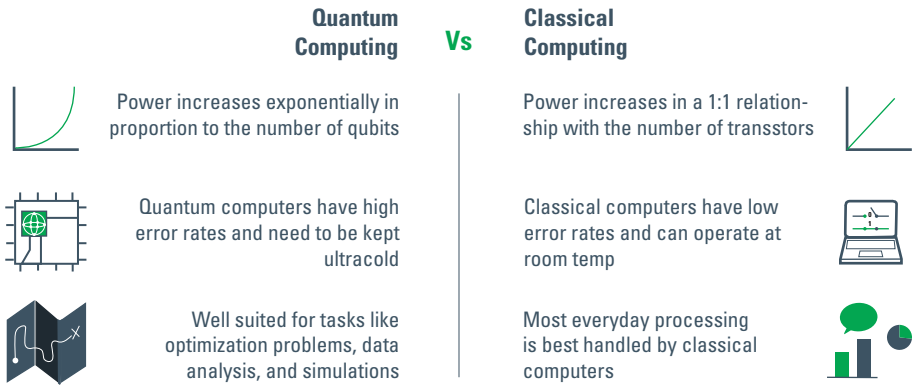

Figura 16: schema riassuntivo delle principali caratteristiche che contraddistingono il Quantum Computing quando comparato al classical computing.[70]

In Figura 16, è possibile ritrovare uno schema che riassume alcune delle principali caratteristiche che distinguono il Quantum Computing dal computing classico.

Questo approccio risulta di particolare efficacia anche in relazione all'Intelligenza Artificiale. Infatti, ad una rete neurale, struttura alla base delle più diffuse IA, può essere affiancata una componente interamente quantistica in grado di aumentare non solo le prestazioni a livello di tempo computazionale, ma anche di avere un impatto positivo sulla accuratezza del risultato - tema particolare sentito nelle applicazioni di Generative AI – grazie alla capacità dell'approccio quantistico di cogliere relazioni tra i dati più complesse rispetto a quanto attualmente possibile. Inoltre, tramite il Quantum Computing, è possibile pensare ad algoritmi di IA completamente basati sulla computazione quantistica in grado di affrontare problemi di classificazione, dall'identificazione della tipologia di documento fino al rilevamento di transazioni fraudolente; ambito in cui questo tipo di tecnologia si è già dimostrata efficace[71].

In conclusione, il settore dei servizi finanziari è uno dei campi di applicazione in cui si intuisce che i vantaggi del Quantum Computing potrebbero essere apprezzati in anticipo rispetto ad altri settori industriali. L'ampio spettro di metodologie già disponibile o in corso di studio corrobora l'idea dell'ingente investimento generale da parte degli enti di ricerca, dei governi e degli stessi istituti finanziari. In una realtà dove la tecnologia si sviluppa con una rapidità senza precedenti, è bene valutare sin da subito l'integrazione di metodologie basate su un approccio rivoluzionario come quello quantistico all'interno dei propri workflow operativi, così da avere consapevolezza dei contesti applicativi che essa stessa abilita e poterne beneficiare progressivamente man mano che essa avanza.

70 Immagine da https://vitolavecchia.altervista.org/differenza-tra-computer-quantistico-e-computer-classico-in-informatica/

71 Liu, Y., Arunachalam, S., Temme, K.: A rigorous and robust quantum speed-up in supervised machine learning. Nature Physics 17(9), 1013–1017 (2021)

IMPATTI DEL QUANTUM COMPUTING NELLA CYBERSECURITY

Il digitale è ormai da considerarsi come un elemento imprescindibile dell'esperienza quotidiana degli utenti in ogni ambito. In particolare, l'accesso e l'utilizzo sempre più frequente di prodotti e servizi finanziari quali home banking e trading online sta spingendo gli enti bancari e assicurativi ad investire significativamente nel loro sviluppo.

Inoltre, la crescente capacità di analisi dati così come il diffondersi dell'intelligenza artificiale permettono alle aziende di concepire e proporre soluzioni innovative e fruibili in mobilità ai propri clienti. Nell'ambito della tecnologia finanziaria digitale (Fintech) è quindi particolarmente importante garantire che tutti gli scambi di informazioni che questi nuovi servizi e prodotti richiedono avvenga in modo intrinsecamente sicuro.

PANORAMICA DELLE METODOLOGIE CRITTOGRAFICHE ATTUALMENTE IN USO

I due principali protocolli crittografici che si sono imposti nell'utilizzo quotidiano sono quelli a chiave simmetrica (o privata) e quelli a chiave asimmetrica (o pubblica).

La crittografia simmetrica codifica e decodifica il dato che si cerca di proteggere facendo uso di un'unica chiave condivisa tra sorgente e destinatario. Ancorché le implementazioni di questo protocollo garantiscano un alto livello di protezione dei dati cifrati e, in generale, una buona velocità di codifica e decodifica, il punto debole della crittografia simmetrica risiede nella gestione delle chiavi che devono essere necessariamente condivise tra chi cifra e chi decifra l'informazione. Per questo la crittografia simmetrica è preferenzialmente utilizzata per proteggere dati at rest piuttosto che dati in motion.

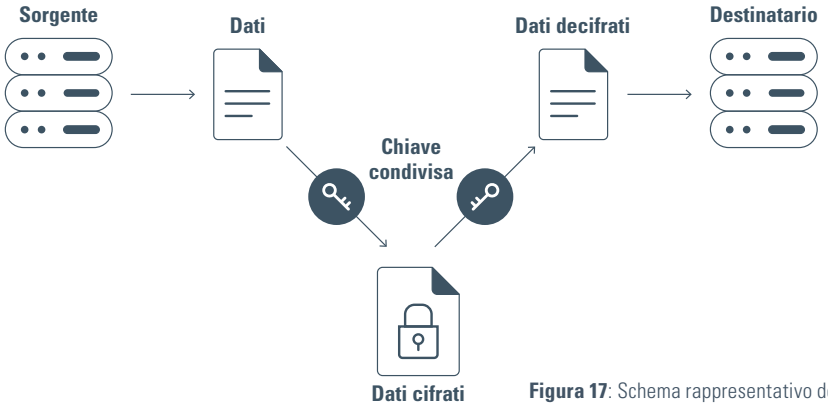

Figura 17: Schema rappresentativo del procedimento di crittografia simmetrica.

La crittografia asimmetrica codifica e decodifica il dato che si cerca di proteggere facendo uso di due chiavi diverse: una pubblica, liberamente condivisa dal sorgente, e una privata in possesso del destinatario. Benché ciò risolva il problema della compromissione derivante da una potenziale non attenta gestione delle chiavi, le implementazioni di questo protocollo sono tipicamente caratterizzate da una minor velocità nei processi di codifica e decodifica, dovuta sia alla maggior lunghezza delle chiavi impiegate, sia alla maggior complessità degli algoritmi impiegati per realizzarli. Per queste ragioni la crittografia asimmetrica è preferenzialmente impiegata per rendere sicure le transazioni finanziarie, le procedure di login e di firma digitale.

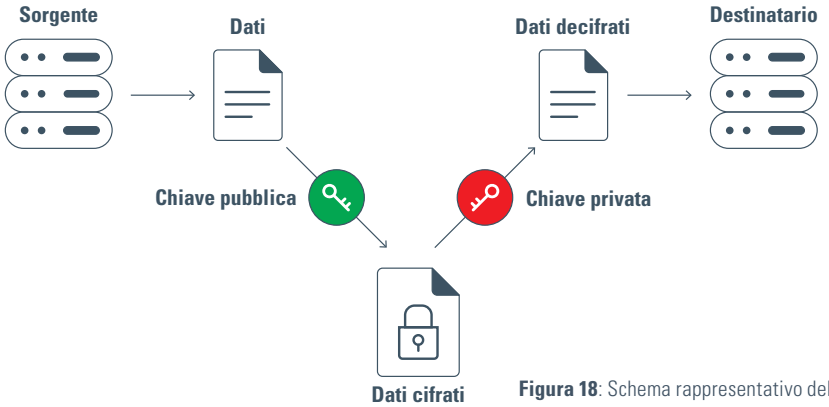

Figura 18: Schema rappresentativo del procedimento di crittografia asimmetrica.

Il concetto di chiave è di particolare interesse nell'ambito della crittografia. Ogni compromissione di una chiave può portare ad una violazione dell'intero sistema. Per questo motivo è necessario regolamentare il sistema di gestione delle chiavi in modo che includa tutte le fasi di utilizzo delle stesse: generazione, conservazione, scambio e sostituzione in caso di compromissione.

La principale tecnica di codifica basata su chiave simmetrica è l'**Advanced Encryption Standard** (AES)[72], sviluppato dal National Institute of Standards and Technology (NIST). Attualmente in uso per la protezione di database governativi, bancari e aziendali, l'AES prevede il trasferimento dell'informazione in blocchi di dimensione predefinita (128 bit), mentre la chiave ha dimensione variabile fino a 256 bit. L'AES si compone di un passaggio preliminare, detto RoundKeyAddition, che combina i byte dei dati con la chiave che si decide di usare. Successivamente, si combinano diversi round per ottenere il dato crittato finale.

La maggior parte dei sistemi per la convalida delle transazioni e quelli di autenticazione si basano sulla crittografia asimmetrica. Primo tra tutti è da citare il sistema di crittografia sviluppato da Ron Rivest, Adi Shamir and Leonhard Adelman (**RSA**)[73]. Tale protocollo si affida alla generale complessità computazionale che la fattorizzazione in numeri primi di un numero comporta.

Un altro schema di cifratura a chiave asimmetrica è quello della crittografia a curve ellittiche (ECC). Questa tipologia di codifica è basata sulla struttura algebrica delle curve ellittiche e sulla generale difficoltà di calcolarne il logaritmo discreto (DLP)[74]. Le cifrature basate sulle curve ellittiche sono alla base dei sistemi di protezione delle firme digitali. Il protocollo ECC è generalmente ritenuto il successore di RSA, poiché permette di usare chiavi più piccole e di effettuare, a parità di dati da cifrare, le operazioni di cifratura e decifratura con maggiore velocità, pur mantenendo elevati standard di sicurezza.

Vista la recente popolarità delle tecnologie per la creazione di registri informativi distribuiti (Distributed Ledger Technologies – DLT) specie in ambito finanziario, è interessante approfondire lo schema crittografico sottostante alla blockchain. La blockchain, inizialmente impiegata per coniare cripto-valute, si compone di tre livelli: uno schema crittografico basato su funzioni di hash e di firma digitale; un protocollo Peer-to-Peer per la comunicazione tra i vari nodi che la compongono; un metodo di convalida delle transazioni condiviso tra i vari utenti. La blockchain è una catena di blocchi di informazione, ciascuno di essi collegato al precedente tramite una codifica, detta hash. Lo schema più diffuso di hash è SHA, con le sue varianti a 256,512 bits. Inoltre, le informazioni di ogni blocco sono organizzate su una struttura dati anch'essa basata sull'hashing, i Merkle trees[75]. Tutte queste caratteristiche contribuiscono ad assicurare le proprietà di trasparenza e tracciabilità delle transazioni che connotano questa tecnologia.

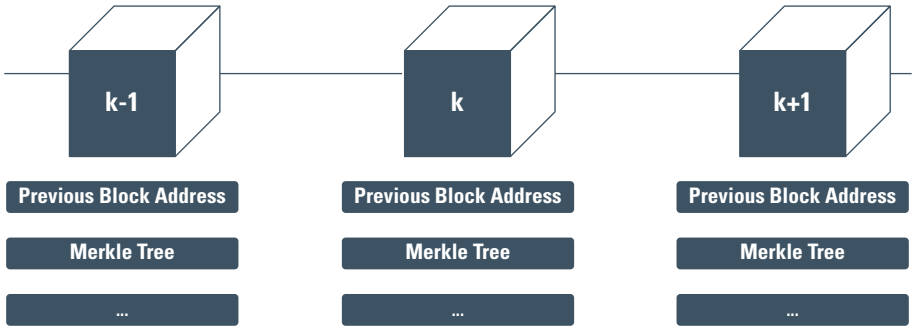

Figura 19: Rappresentazione schematica della struttura dati legata ai Merkle trees.

72 Joan Daemen and Vincent Rijmen, AES proposal: Rijndael, 1999. Gaithersburg, MD, USA

73 Milanov, Evgeny. "The RSA algorithm." RSA laboratories (2009): 1-11.

74 McCurley, Kevin S. "The discrete logarithm problem." Proc. of Symp. in Applied Math. Vol. 42. 1990.

75 Becker, Georg. "Merkle signature schemes, merkle trees and their cryptanalysis." Ruhr-University Bochum, Tech. Rep 12 (2008): 19.

LA MINACCIA DEL QUANTUM COMPUTING

Dalla sezione precedente, si evince come molte delle metodologie su cui si basano gli attuali sistemi di protezione dati dipendano dalla generale assunzione di intrattabilità di particolari problemi matematici in tempi utili, immaginando di risolverli con gli attuali elaboratori. Stante la loro potenziale miglior capacità computazionale, i computer quantistici potrebbero in futuro intaccare quindi la sicurezza alla base dei protocolli a chiave asimmetrica e delle funzioni hash (lo schema crittografico alla base delle blockchain), nonché indebolire i sistemi a chiave simmetrica.

Di seguito si riportano le risorse che il Global Risk Institute[76][77] stima siano necessarie a violare i principali sistemi di crittografia oggi in uso. Nella tabella, la colonna "Sicurezza" si riferisce al numero n di bit classici impiegati per implementare l'algoritmo: si tenga presente che il numero di bit necessari per violare tale codifica con un elaboratore classico sono circa 2^n

Codifica	Sicurezza	Qubit necessari	Tempo di risoluzione
Rsa-3072	128 bits	12290	35.4 minuti
Rsa-4096	156 bits	16386	70.2 minuti
Rsa-7680	192 bits	30722	5.93 ore
NIST P-256	128 bits	2330	10.5 ore
NIST P-521	260 bits	4959	95 ore

È interessante notare come le procedure di codifica basate su chiave simmetrica siano meno soggette ad una compromissione della loro sicurezza da parte di algoritmi quantistici nel breve e medio periodo. Infatti, le stime condotte rispetto a questi schemi di cifratura ritengono necessario l'impiego di un numero di qubit significativamente maggiore rispetto alle numeriche riportate nella tabella precedente.

Risulta dunque evidente come esista un concreto rischio per la sicurezza delle informazioni legato all'avvento del quantum hardware.

76 Gheorghiu, Vlad and Michele Mosca. "A Resource Estimation Framework For Quantum Attacks Against Cryptographic Functions: Recent Developments." (2020).

77 Gheorghiu, Vlad and Michele Mosca. "A resource estimation framework for quantum attacks against cryptographic functions GRI quantum risk assessment report." (2017).

POSSIBILI ALTERNATIVE QUANTUM-SAFE E QUANTUM-PROOF ROADMAP

In un periodo in cui potenziare la sicurezza digitale risulta nuovamente necessario e in analogia con quanto precedentemente fatto nel corso degli anni '90, il NIST ha annunciato nel 2016 la competizione Post-Quantum Cryptography Standardization per trovare nuovi algoritmi di cifratura standard nell'era post-quantum. Nel luglio del 2022 si è concluso il terzo di quattro round previsti con la pubblicazione dei migliori algoritmi candidati finora identificati. Nel documento[78] si evidenziano **CRYSTAL-Kyber, CRYSTAL-Dilithium, Falcon and SPHINCS**$^+$ come nuovi standard e si rimandano altri quattro algoritmi al quarto round per ulteriore analisi. In modo particolare, il NIST segnala CRYSTAL-Dilithium come primo schema crittografico da sviluppare nell'ambito della firma multipla. CRYSTAL-Kyber[79] è invece un insieme di codifiche quantistiche basato su un meccanismo di incapsulamento delle chiavi (KEM) per la cifratura asimmetrica.

Le principali categorie di algoritmi evidenziati nella crittografia post-quantum sono: **Lattice-based, Hash-based, Code-based, Multivariate-based**.

La crittografia basata sui reticoli (lattices) è stata inizialmente proposta da Ajtai e Dwork[80]. Gli algoritmi lattice-based trovano fondamento sulla generale difficoltà di risolvere problemi basati proprio sulla struttura di reticolo, oggetto matematico appartenente all'algebra lineare. Un esempio è il problema del vettore minimo (SVP)[81]. La più tradizionale crittografia ad hash prevede invece che una stringa venga mappata in una sequenza binaria di lunghezza fissa.

Gli schemi di cifratura code-based si basano sull'applicazione di codici di correzione d'errore ai dati oggetto di cifratura. Queste tecniche hanno il vantaggio di poter gestire chiavi di lunghezza maggiore garantendo comunque prestazioni di cifratura rapide, rappresentando una valida alternativa alle implementazioni lattice-based.

La crittografia Multivariate-based fa invece uso di algoritmi basati sulla difficoltà di risolvere sistemi di equazioni polinomiali multivariate in un campo finito.

Si riporta in seguita una tabella riassuntiva dei principali algoritmi post-quantum nello scenario attuale.

	Lattice	**Hash**	**Code**	**Multivariate**
Algoritmi	– CRYSTAL-Kyber – CRYSTAL-Dilithium – Falcon	– SPHICS$^+$	– BIKE	– Rainbow
Vantaggi	– Gestione delle chiavi molto veloce – Implementazione relativamente semplice	– Chiavi pubbliche corte – Solida sicurezza	– Solida sicurezza	– Piccole firme – Procedure di verifica della firma veloce

Un metodo rilevante per la sicurezza delle comunicazioni è la Quantum key distribution (QKD)[82]. QKD è un protocollo di comunicazione dati basato sul principio di entanglement in virtù del quale rende sia impossibile ad un eventuale terza persona (eavesdropper) in ascolto sul canale di comunicazione tra sorgente e destinatari di carpire informazioni, sia al destinatario di rilevare il tentativo di intercettazione.

78 https://csrc.nist.gov/publications/detail/nistir/8413/final

79 J. Bos et al., "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 2018, pp. 353-367, doi: 10.1109/EuroSP.2018.00032.

80 Ajtai, Miklós, and Cynthia Dwork. "A public-key cryptosystem with worst-case/average-case equivalence." Proceedings of the twenty-ninth annual ACM symposium on Theory of computing. 1997.

81 Stehlé, D., Steinfeld, R., Tanaka, K., & Xagawa, K. (2009). Efficient Public Key Encryption Based on Ideal Lattices. Cryptology ePrint Archive, Paper 2009/285. https://eprint.iacr.org/2009/285

82 The security of practical quantum key distribution Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev Rev. Mod. Phys. 81, 1301 – Published 29 September 2009

Il protocollo QKD è usato anzitutto per produrre una chiave casuale, tramite l'utilizzo di un apposito generatore quantistico di numeri casuali (Quantum Random Number Generator – QRNG), e poi per distribuirla su un canale di comunicazione quantistico inattaccabile. La QKD è impiegata per realizzare protocolli crittografici a chiave simmetrica, come l'Advanced Encryption Standard (AES). In Figura 20 è possibile trovare uno la rappresentazione schematica del protocollo.

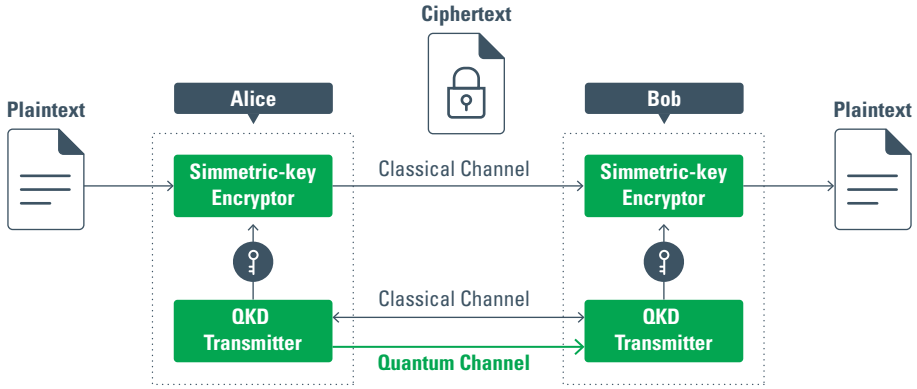

Figura 20: Schema di cifratura basato su QKD.[83]

La sicurezza delle chiavi generate e scambiate con QKD, basandosi su un principio fisico quantistico piuttosto che sulla difficoltà di risolvere un certo problema matematico pur complesso, è in modo intrinseco quantum-proof.

Trattandosi di una tecnologia commercialmente disponibile ormai da alcuni anni, alcune BigTech e importanti gruppi industriali hanno già superato la fase di sperimentazione della QKD preparandosi a renderla produttiva nel breve periodo.

Emerge, quindi, la fondamentale importanza di condurre un **Quantum Risk Assessment**. Il lavoro pubblicato dal Global Risk Institute rappresenta una visione chiara di quelle che sono le minacce date dall'avvento di tecnologie quantistiche in tutti i campi, in modo particolare in quello finanziario dove la sicurezza dei dati sensibili ricopre un ruolo centrale. I principali protocolli oggi utilizzati per garantire la sicurezza delle transazioni e dei sistemi di autenticazione sono messi a rischio dalle capacità di calcolo che si ipotizza i futuri dispositivi quantum saranno in grado di esprimere. Un'ulteriore minaccia deriva dalla percezione che si tratti esclusivamente di una minaccia futura. Tuttavia, i dati cifrati con le tecniche classiche, qualora esfiltrati, potrebbero essere facilmente codificati in un futuro prossimo, mediante i cosiddetti retroactive attacks. L'investimento culturale e finanziario nel rafforzamento della cybersecurity risulta dunque una strada da percorrere sin d'ora. In tal senso, è una buona prassi condurre un risk assessment che restituisca una mappatura sistemica delle tecniche di cifratura usate nei vari sistemi informatici a protezione dei propri dati, in modo da evidenziare eventuali debolezze ed essere a conoscenza di quando e quali protocolli sostituire con i loro corrispettivi quantum-proof.

In definitiva, emerge ormai in tutti i principali tavoli di confronto la necessità di adoperarsi in uno sforzo collettivo europeo che integri le prassi descritte per la quantum-proof roadmap nei principali quadri normativi che regolano la sicurezza informatica e la protezione dei dati.

83 Immagine presa da Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, Secondquarter 2022, doi: 10.1109/COMST.2022.3144219.

CONCLUSIONI

L'esplorazione delle tecnologie quantistiche ha evidenziato l'enorme potenziale del Quantum Computing per il mondo dei servizi finanziari.

Passando dalla presentazione dei dispositivi attualmente in sviluppo agli algoritmi già implementati, il presente documento aiuta a prendere coscienza delle possibili integrazioni del Quantum Computing nei propri flussi di lavoro operativi. La portata di questa tecnologia non risiede solo nella sua componente applicata a tecniche di analisi e predizione dei dati, ma anche in larga parte al suo impiego nel campo della sicurezza delle informazioni. Si è dato risalto sia a come l'integrazione delle procedure quantistiche in algoritmi classici potrebbe snellirne il carico computazionale, sia come sia in atto una competizione per il raggiungimento di nuovi standard di crittografia resilienti in una futura era post-quantum.

Le metodologie e le implicazioni derivanti dall'applicazione delle tecnologie quantistiche portano con sé anche un potenziale miglioramento della qualità percepita e della capacità dei servizi offerti agli utenti finali. Si pensi, ad esempio, a come una più accurata e rapida pianificazione dell'utilizzo della rete di comunicazione dei telefoni cellulari possa avere impatto nella qualità del servizio che l'utente percepisce o come una maggior efficacia negli algoritmi per la definizione dei percorsi rapidi dei più diffusi navigatori possa ridurre i tempi di percorrenza ed i livelli di traffico urbano. Inoltre, si pensi ai benefici indiretti che un consumatore finale potrebbe sperimentare, come la potenziale velocizzazione della messa in commercio di nuovi farmaci grazie alle simulazioni quantistiche sulle molecole. Ultimo, in relazione sempre all'ambito finanziario, migliori applicazioni dei sistemi di previsione del mercato, o di tecniche di contenimento del rischio di investimento, potrebbero portare ad un guadagno maggiore per l'investitore privato e per l'istituto finanziario.

Dal punto di vista entreprise, il Quantum Computing, dato il suo potenziale impatto su tecnologie e servizi attualmente in uso nelle aziende, potrà comportare una completa rivisitazione dei processi decisionali. L'adozione di algoritmi caratterizzati da una tecnologia sottostante così diversa renderà, infatti, necessario un processo di adozione incrementale ma diffuso, in modo da garantire la competitività nei confronti dei player che svilupperanno o acquisiranno rapidamente know-how su di essa. Da un punto di vista pratico, risulta quindi di fondamentale importanza avere personale istruito sulle peculiarità che contraddistinguono questa tecnologia, così da poterne comprendere opportunità e rischi.

Volgendo lo sguardo allo sviluppo sistemico con riferimento al mandato di Cassa Depositi e Prestiti, risulta già chiaro come la definizione ed implementazione da parte degli attori istituzionali di una strategia che sia in grado di legare ricerca, investimenti pubblici e privati ed esigenze del mercato sarà cruciale per cogliere un'opportunità senza precedenti. Oltre alle analogie con gli exploit passati di tecnologie ormai più che diffuse come Cloud ed Intelligenza Artificiale, è possibile citare alcuni comportamenti esemplificativi. Primo fra tutti, il governo tedesco che, impegnato a mantenere la propria posizione di leader nella corsa globale per la tecnologia quantistica, sta investendo attivamente nella ricerca, nello sviluppo e nella commercializzazione in questo campo. Se da un lato questo ha infatti distribuito chiari mandati a diversi istituti di ricerca e centri di eccellenza come, ad esempio, quello all'Istituto Fraunhofer per la ricerca sulla crittografia e su altri aspetti della sicurezza quantistica e quello per l'ottica quantistica e per la scienza dell'informazione quantistica al Max Planck Institute, dall'altro il Ministero federale per gli affari economici metterà a disposizione circa 740 milioni di euro al Centro aerospaziale tedesco (DLR) per finanziare un progetto di calcolo quantistico basato su trappole ioniche. Degno di nota è anche l'investimento nello sviluppo di hardware per il calcolo quantistico per fornire risorse all'ecosistema di startup e piccole e medie imprese. Con una finalità simile a quest'ultima citata per il caso tedesco, nella primavera del 2022, il governo giapponese ha dichiarato un ulteriore investimento di 4,2 miliardi di yen (circa 32 milioni di dollari) per sostenere l'espansione dello Shared Quantum Computing (già realizzato) attraverso piattaforma cloud. L'azione si inserisce all'interno del piano aggiornato attraverso cui il governo nipponico ha formulato una nuova strategia quantistica, denominata Vision of Quantum Future Society, che mira ad incorporare la tecnologia quantistica nei sistemi sociali ed economici, nonché a creare opportunità di sostenibilità.

In definitiva, sebbene le tempistiche di adozione risultino ancora incerte, gli investimenti attualmente in corso e futuri promettono uno sviluppo ancor più rapido delle capacità dei dispositivi quantum. Proprio per questo, risulta necessario che si ponga la dovuta attenzione su quest'ambito sin da subito, in modo da non rimanere irrimediabilmente svantaggiati in un contesto dove diversi attori hanno già palesato le proprie ambiziose intenzioni ed hanno avviato, o stanno per avviare, importanti filoni di ricerca e sviluppo.