CONVENZIONE INTERBANCARIA
PER L'AUTOMAZIONE
(CIPA)

Le tecnologie quantistiche nel settore bancario

Maggio 2024

La Segreteria Tecnica della Convenzione desidera ringraziare i componenti del gruppo di lavoro, di seguito indicati, per la collaborazione prestata e il contributo fornito nello svolgimento delle attività del gruppo.

Elena	BUCCIOL	Banca d'Italia (Coordinatrice)
Katia	BORIA	Banca d'Italia - Segreteria Tecnica CIPA
Matteo	ELIA	Banca d'Italia - Segreteria Tecnica CIPA
Domenico	PETRUCCIANI	Banca d'Italia - Segreteria Tecnica CIPA
Mario	TRINCHERA	ABI Lab
Ivan Luciano	DANESI	UniCredit
Lorenzo	DEMELAS	UniCredit
Davide	CORBELLETTO	Intesa Sanpaolo
Dimitar	ANASTASOVSKI	Sella
Stefano	PRIOLA	Sella
Matteo	BALBONI	Banco BPM
Gloria	MASSERA	Banco BPM

Si ringraziano, altresì, Cristina Andriani, Giuseppe Bruno, Angelo Germoni e Pietro Tiberi della Banca d'Italia per la collaborazione utile per l'approfondimento di alcuni aspetti trattati, Marina Natalucci, dell'Osservatorio "Quantum computing & communication" del Politecnico di Milano, per la disponibilità a condividere i dati della rilevazione, il cui copyright © è in capo al DIG – Dipartimento di Ingegneria Gestionale del Politecnico di Milano, di cui sono riportati riferimenti al capitolo 4.4.

Indice

1 Premessa

Le tecnologie quantistiche, ovvero quell'insieme di componenti hardware e software che sfrutta le leggi della meccanica quantistica per trattare oggetti su scala atomica e subatomica, rappresentano uno dei fenomeni emergenti più interessanti del panorama dell'Information Technology (IT) di questi ultimi anni.

L'obiettivo di questo documento è sensibilizzare il mondo bancario e finanziario alle opportunità e ai rischi connessi con il loro avvento e offrire una base comune di conoscenze per intraprendere iniziative e avviare strategie.

A differenza di molti aspetti dell'IT, l'approfondimento di questi temi risulta inscindibile dalla conoscenza della teoria fisica sottostante che descrive con successo da più di un secolo il comportamento di fenomeni a livello microscopico. Inoltre, l'approccio ad alcuni temi, come gli algoritmi utilizzabili con gli elaboratori quantistici o i principi alla base della crittografia, richiede competenze nell'ambito dell'algebra lineare e della matematica avanzata. Tuttavia, la lettura di un documento che riporti continui riferimenti a dettagli specifici della teoria, risulterebbe piuttosto faticosa. Si è perseguito, pertanto, uno sforzo di astrazione che consenta di cogliere gli aspetti principali di questo nuovo e stimolante contesto, inserendo alcuni riferimenti per approfondire singoli aspetti.

Il presente documento, redatto nei primi mesi del 2024, non ha pretese di essere esaustivo; è frutto degli approfondimenti e del confronto degli autori sugli argomenti trattati, nonché delle esperienze acquisite durante il corso del proprio esercizio professionale.

Ai fini della stesura del resoconto, il gruppo di lavoro si è avvalso di differenti fonti: dati e informazioni rese pubbliche dagli analisti e dalla stampa specializzata, risorse messe liberamente a disposizione dal mondo della ricerca scientifica e dell'industria, siti web dei fornitori di tecnologia e consulenza.

La disponibilità delle pagine web, di cui sono riportati i riferimenti nel testo, è stata verificata alla data di stesura di questo documento (maggio 2024).

Le opinioni espresse in questo resoconto descrivono il punto di vista degli autori e non necessariamente riflettono quelli delle rispettive Istituzioni che rappresentano.

2 Introduzione

Il complesso di intuizioni, interpretazioni e modelli matematici nati a partire dall'inizio del '900 per la descrizione dei fenomeni su scala atomica, che va sotto il nome di meccanica quantistica, rappresenta, nella storia del progresso scientifico, uno dei successi più sorprendenti sul piano predittivo e su quello delle implicazioni pratiche. La tecnologia digitale che ci è familiare, con la quale ci misuriamo quotidianamente e che facilita, ad esempio, la scrittura e la diffusione di documenti come il presente resoconto, è basata proprio su dispositivi realizzati grazie alla scoperta delle leggi della meccanica quantistica. In particolare, l'introduzione della fisica dei semiconduttori per la costruzione di componenti come transistor, laser e altri elementi elettronici viene considerata parte di quella che va sotto il nome di "prima rivoluzione quantistica". Gli aspetti che sono oggetto di questa trattazione (il quantum *computing*, la crittografia quantistica, il quantum *sensing*), invece, fanno parte della cosiddetta "seconda rivoluzione quantistica" nella quale si sfruttano caratteristiche (come sovrapposizione ed *entanglement* di stati fisici) riferite al comportamento di singole particelle subatomiche.

La peculiarità del comportamento degli oggetti microscopici ha reso prima ipotizzabile, a partire dagli anni '80, e poi realizzabile, grazie a continui avanzamenti tecnologici, la progettazione di dispositivi in grado di abilitare un nuovo paradigma di calcolo completamente diverso da quelli noti nell'informatica teorica classica, basata sull'algebra booleana (dove l'unità informativa, il bit, può assumere i valori "0" e "1"). Gli elaboratori quantistici sfruttano, infatti, la proprietà di oggetti microscopici (*qubit*) di poter assumere differenti valori (formalmente "0" e "1") "allo stesso tempo" e offrire, in un certo modo, un grado di parallelismo che trova differenti applicazioni. In particolare esso si tradurrebbe, raggiunta una certa maturità tecnologica, in un incremento sostanziale della capacità di calcolo che consentirebbe la risoluzione di alcuni problemi considerati intrattabili dall'informatica classica. Da questo punto di vista, al pari di altre tecnologie, la computazione quantistica potrebbe diventare patrimonio dell'umanità a beneficio di ricerca e sviluppo nel campo della salute, dell'ambiente e dell'intelligenza artificiale.

La realizzazione pratica di questo paradigma di calcolo, a causa della complessità che comporta la gestione di particelle microscopiche[1], è, al momento, lontana dall'essere definita, nonostante gli investimenti ingenti da parte di molti grandi imprese commerciali. In particolare, l'attuale offerta tecnologica rientra nel novero dei "*Noise Intermediate Scale Quantum*" (NISQ), con la presenza di un numero limitato di *qubit* definiti "rumorosi" per la loro instabilità e senza un meccanismo affidabile di correzione degli errori dovuti alla difficoltà di mantenere la coerenza tra gli stati quantistici. Nel lungo termine, l'obiettivo è di avere dei dispositivi "*fault-tolerant*" (FTQC), anche detti computer quantistici "universali", che consentano la piena realizzazione del nuovo modello di calcolo.

Nel frattempo, sono state avviate diverse iniziative per identificare differenti campi in cui l'introduzione di questo nuovo approccio potrebbe apportare reali benefici. A partire dagli anni

[1] Esiste inoltre un intero ambito di studio, di cui non si fa cenno in questa relazione, dedicato alle tecnologie "abilitanti" per il quantum *computing*: criogenia, elettronica, laser, sorgenti e rilevatori di fotoni, produzione di specifici materiali con proprietà quantistiche.

novanta, prima ancora che grandi aziende cominciassero la progettazione di questi dispositivi, sono stati sviluppati algoritmi quantistici per l'ottimizzazione di alcuni problemi, noti dalla teoria della complessità computazionale, come quello della ricerca di un elemento in uno spazio non strutturato o quello della fattorizzazione degli interi.

Tuttavia, la disponibilità di elaborazione quantistica sufficiente a garantire l'esecuzione di questi algoritmi su vasta scala pone una seria minaccia[2] ai sistemi crittografici alla base della sicurezza dell'universo cibernetico in cui tutti i giorni circolano dati sensibili, transazioni economiche e segreti militari.

Per far fronte a queste minacce, sono state individuate due strategie principali. La prima consiste nell'utilizzo, nella cifratura, di problemi di matematica classica per i quali, al momento, non esiste un algoritmo quantistico che consenta la loro violazione. La seconda sfrutta a sua volta alcune proprietà della meccanica quantistica nella costruzione di dispositivi ottici (emettitori e rivelatori di fotoni) che consentano lo "scambio" di informazioni (in particolare le chiavi di cifratura) in modo completamente sicuro.

Anche se gli elaboratori quantistici disponibili non sono, allo stato attuale, in grado di violare i meccanismi alla base della crittografia tradizionale, i dati che necessitano di essere mantenuti confidenziali per un lungo periodo potrebbero essere già esposti al rischio poiché cyber criminali potrebbero essersene impossessati e conservarli in attesa di avere a disposizione gli strumenti per violarli ("*store now, decrypt later*"). Inoltre, il problema di violazione riguarda anche la firma digitale e la compromissione della validità di documenti già firmati per i quali è necessaria l'introduzione di un sistema di garanzia come l'infrastruttura a chiave pubblica (PKI) valido anche nell'era "post-quantum".

Questo contesto diventa particolarmente importante se si guarda al mondo finanziario per la crescente digitalizzazione e interconnessione e per il fatto di essere crescente bersaglio di attacchi informatici[3]. In attesa del "*Q-day*"[4], è necessario programmare il prima possibile una valutazione del patrimonio di dati sensibili e critici all'interno di ciascuna organizzazione e del loro trattamento per l'introduzione di una strategia quantum *safe*[5].

[2] Nel 1995, il matematico dei Bell Lab Peter Shor ha dimostrato che il problema di fattorizzazione degli interi, la cui complessità è una delle basi della crittografia moderna, è "risolvibile" con un computer quantistico sufficientemente potente, utilizzando un algoritmo quantistico, in tempi decisamente inferiori (dell'ordine di minuti) rispetto a quelli richiesti dall'elaborazione classica (paragonabili ai tempi di vita dell'universo).

[3] I dati del recente rapporto Clusit 2023 mostrano non solo che nell'ultimo quinquennio il settore finanziario e assicurativo si trovi tra i principali bersagli per numerosità degli attacchi (10,5%) e per impatto degli stessi (40% degli attacchi ritenuti critici) ma anche che questo dato sia costantemente in crescita.

[4] Si definisce con "Q-day" il momento in cui sarà disponibile un elaboratore in grado di compromettere gli attuali sistemi di crittografia basati su chiave pubblica (ad es. RSA-2048).

[5] Per fornire qualche esempio: la migrazione da SHA-1 a SHA-2 ha richiesto approssimativamente 10 anni. Blackberry ha impiegato cinque anni per migrare da 3DES a AES, pur avendo il controllo di tutti i *device* e server. MD5, nonostante le note vulnerabilità, risulta ancora utilizzato in alcuni contesti (CARAF: Crypto Agility Risk Assessment Framework | Journal of Cybersecurity | Oxford Academic (oup.com) https://doi.org/10.1093/cybsec/tyab013).

Il mercato offre già oggi molte opportunità sia per sperimentare le possibilità offerte dal calcolo quantistico[6], sia per introdurre elementi di sicurezza quantum *safe* nelle infrastrutture informatiche. Nel mondo bancario e finanziario, una grossa parte delle sperimentazioni in corso e delle applicazioni sono legate a modelli per la risoluzione di problemi che trovano applicazione in tale settore e ne rappresentano il core business come la stima del rischio di credito e l'ottimizzazione del portafoglio.

Il campo delle tecnologie quantistiche vede, dall'ultimo decennio, l'intervento di rilevanti investimenti, anche da parte di governi nazionali e sovranazionali: la Cina da sola ha annunciato l'investimento di più di 15 miliardi di dollari, ma anche l'Europa rappresenta la seconda area geopolitica per investimenti pubblici[7]. La Commissione europea, in particolare, ha stanziato investimenti per un piano di lunga durata per coordinare le differenti attività tra istituti di ricerca, industria ed enti pubblici. In ambito nazionale vi sono diverse iniziative seppure l'investimento sia limitato (1,6 miliardi di euro all'interno del Piano Nazionale di Ripresa e Resilienza - PNRR per temi tecnologici di importanza critica, tra cui anche il quantum *computing*).

La natura dei temi legati alla tecnologia quantistica è estremamente complessa: da una parte le conoscenze necessarie al suo sviluppo e, talvolta, persino al suo utilizzo sono legate all'ambito scientifico e richiedono una ricerca di tipo accademico, dall'altra i costi necessari per l'adozione di queste tecnologie sono elevati e richiedono di pianificare un ritorno di investimento protratto nel tempo. Si assiste a una crescita di start up innovative che offrono servizi di varia natura, all'aumento dell'offerta formativa in questi ambiti e alla redazione di piani di strategia nazionali per lo sviluppo di questo settore. L'interesse verso queste tecnologie coinvolge numerosi attori da quelli privati a quelli istituzionali, fino a enti e organizzazioni internazionali: è necessaria una collaborazione stringente, di cui questo stesso documento si fa promotore, tra queste realtà per individuare una strategia comune, in particolare per i temi legati alla sicurezza dei dati e delle comunicazioni.

Alcuni settori applicativi, in particolare quelli concernenti la sicurezza, possono trarre maggiori opportunità da soluzioni quantistiche. Altri ambiti, quali ad esempio il *machine learning*, possono egualmente beneficiarne, ma in un'ottica di medio lungo periodo; ciò dipende dalla maturità della ricerca scientifica e dalla disponibilità di tecnologia a costi accessibili. In virtù di tali considerazioni questo rapporto approfondisce maggiormente i temi legati alla sicurezza- come la protezione delle comunicazioni e la salvaguardia dell'integrità dei dati, che sono interessati dall'avvento delle tecnologie quantistiche in un'ottica di breve periodo – e tratta con un minor grado di dettaglio gli ambiti legati al business o ai modelli di *machine learning*, in quanto questi ultimi sono ancora agli inizi della rivoluzione tecnologica quantistica.

Il presente lavoro è organizzato in capitoli tematici per guidare il lettore a una comprensione generale del funzionamento delle tecnologie quantistiche, delle sue implementazioni e delle possibili strategie di adozione. Dopo un approfondimento sulla meccanica quantistica, nel capitolo 3 si affrontano le principali applicazioni, sia in ambito della sicurezza, sia in quello delle possibili

[6] È possibile accedere a risorse quantistiche con modalità simili a quelle della computazione tradizionale, ossia tramite API verso sistemi in cloud, utilizzando dei kit di sviluppo software che consentono di compilare del codice e "lanciarlo" su piattaforme quantistiche. In base ad alcune stime il mercato del quantum *computing* "*as a service*" potrebbe raggiungere i 26 miliardi di dollari nel 2030 (https://thequantuminsider.com/about-us/).

[7] https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

applicazioni di business. Il capitolo 4 è dedicato all'approfondimento delle peculiarità dell'ecosistema che ruota attorno alla tecnologia: la ricerca, il coinvolgimento delle istituzioni, gli investimenti associati, il mercato. Si è deciso di dedicare un intero capitolo (capitolo 5) alle strategie di quantum *safety* per sottolineare l'importanza del tema. Nel capitolo 6 si propone un approfondimento sugli impatti e le possibilità generati dalle tecnologie quantistiche con il focus sulle esigenze dell'ambito bancario. Il lavoro termina con una riflessione, condivisa dal gruppo di lavoro, sugli argomenti trattati e sulle indicazioni che emergono per affrontare questo tema di impatto globale.

3 La meccanica quantistica e le sue applicazioni nell'IT

3.1 Cenni di meccanica quantistica

La fisica classica è un modello che descrive un mondo dove gli "oggetti" possiedono proprietà macroscopiche (posizione, velocità, ecc.) che possono essere misurate con precisione arbitraria, fissato un sistema di riferimento. L'evoluzione di un dato sistema fisico, note le condizioni iniziali, è quindi univocamente determinata dalla risoluzione di equazioni ricavate dalle leggi fisiche.

Quando la dimensione degli oggetti si riduce alla scala subatomica, la fisica classica non è più adatta a descriverne il comportamento e si ricorre alla meccanica quantistica. Quest'ultima prevede l'esistenza di entità che non possiedono valori definiti per le proprietà fisiche (cosiddette "stati").

L'operazione di misura dello stato di queste entità assume un ruolo fondamentale: prima della misura, infatti, esse si possono trovare in una configurazione in cui possiedono "contemporaneamente" tutti i loro possibili stati ("sovrapposizione di stati"). La misura fa manifestare solo uno dei possibili stati con una definita probabilità. Ad esempio, il quanto di luce, il fotone, possiede una proprietà (polarizzazione) che determina il suo comportamento nell'attraversare o meno un filtro polarizzatore orientato. Un fotone polarizzato a 90° (verticale) ha il 100% di probabilità di attraversare un filtro orientato lungo lo stesso asse e 0% di probabilità di attraversare un filtro a 0° (orizzontale). Nel caso, tuttavia, si utilizzi un filtro a polarizzazione differente (45° per esempio), lo stesso fotone polarizzato verticalmente ha il 50% di probabilità di attraversare il filtro (e il 50% di non attraversarlo) e, sorprendentemente, acquisire la rispettiva proprietà (polarizzazione a 45°) a causa della misura stessa.

Il computer quantistico codifica informazioni proprio nelle proprietà di alcuni di questi oggetti subatomici, come elettroni o fotoni, che possono essere sfruttati per risolvere alcuni problemi computazionali in modo estremamente più veloce rispetto ai computer tradizionali.

Il computer classico ha come componenti fondamentali i bit ("0" o "1"), il computer quantistico utilizza i *qubit*, realizzati tramite oggetti che possono essere preparati in sovrapposizione di stati (legati, ad esempio, ad alcune caratteristiche delle particelle elementari, come la polarizzazione dei fotoni) e che, quindi, hanno solamente una definita probabilità di essere "0" oppure "1".

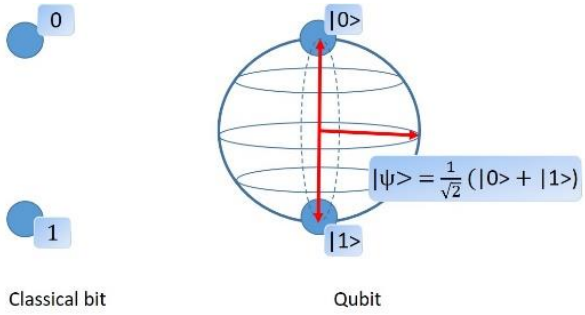


Figura 1: Classical bit e *Qubit*[8] – Nella descrizione classica dei fenomeni, il valore di una data proprietà fisica (ad esempio la posizione) può essere identificato univocamente (ad esempio "0" per la posizione "in alto" e "1" per quella "in basso"). Per realizzare i *qubit*, invece, si sfruttano le proprietà quantistiche delle particelle subatomiche di poter essere preparate in modo tale da trovarsi "in sovrapposizione coerente di stati", ovvero trovarsi in uno stato (normalmente identificato con la notazione di Dirac |ψ>) corrispondente alla sovrapposizione lineare di più stati di base (|0> e |1>) corrispondenti ai valori "0" e "1". I coefficienti della composizione lineare di questi stati (nell'esempio in figura $1/\sqrt{2}$) sono legati alla probabilità (in questo caso ½) di trovare la particella nello stato di base corrispondente nel momento in cui sia effettuata una operazione di misura su di essa.

Questa proprietà di essere "0" e "1" allo stesso tempo implica la possibilità di utilizzare nel calcolo, combinando diversi *qubit*, una forma di parallelismo che, per determinati problemi, tramite la sequenze di un certo numero di operazioni (algoritmi), consente di arrivare più rapidamente alla soluzione. Un sistema costituito da due *qubit* in sovrapposizione di stati è, infatti, in grado di immagazzinare la stessa informazione (sfruttando le possibili combinazioni 00, 01, 10 e 11) di 4 bit classici: n *qubit* corrispondono a 2^n bit classici.

Gli algoritmi quantistici e i protocolli di comunicazione quantistica utilizzati per lo scambio di messaggi cifrati sfruttano anche un altro fenomeno privo di analogo nella fisica classica, l'*entanglement*. Grazie a questo, in determinate condizioni, i valori di una proprietà di due o più sistemi che interagiscono non può essere descritta separatamente ma risulta correlata in modo tale che la misura su uno dei sistemi influenzi, anche ad arbitraria distanza, l'esito della misura sull'altro.

Ad esempio, è possibile manipolare due fotoni per realizzare uno stato fisico che risulti nella sovrapposizione di stati in cui i due fotoni sono entrambi polarizzati orizzontalmente oppure entrambi polarizzati verticalmente. In questo caso i fotoni non solo non possiedono più alcun valore definito di polarizzazione, ma la misura del valore dell'uno farebbe acquisire un valore anche all'altro senza che vi sia stata nessuna interazione diretta con esso.

Questa proprietà può essere sfruttata e trasmessa rendendo possibile l'esecuzione di algoritmi che non trovano analogo nel mondo classico.

3.2 Quantum *Computing*

Nel 1982 il fisico premio nobel Richard Feynman ipotizzò la possibilità di sfruttare le caratteristiche della meccanica quantistica per la realizzazione di elaboratori rilevando come un ipotetico

[8] Tratta da: https://w3.lnf.infn.it/computer-quantistici-verso-la-qubit-generation/. La notazione di Dirac |0> e |1> indica i possibili stati della particella, legati ai valori associati a una determinata proprietà fisica: ad esempio |0> potrebbe corrispondere a un fotone polarizzato orizzontalmente e |1> a uno polarizzato verticalmente.

calcolatore quantistico avrebbe potuto costituire un vero e proprio simulatore della teoria, ovvero, nel corso del suo funzionamento, avrebbe di fatto potuto eseguire degli esperimenti quantistici.

A partire dagli anni '80 è iniziato un lungo percorso, di cui i nostri tempi sono parte, per l'identificazione della tecnologia con cui costruire questo tipo di elaboratori. In parallelo, gli studi si sono concentrati su algoritmi che non si basassero sull'adattamento di quanto impiegato nei calcolatori classici, ma sfruttassero questa nuova modalità di elaborazione e le caratteristiche intrinseche dei sistemi quantistici.

Le esigenze indirizzate da questo nuovo paradigma di calcolo possono essere sintetizzate nelle seguenti:

- effettuare alcuni calcoli basati su problemi più complessi, classicamente intrattabili[9], di quelli che si riescono oggi a fare con i computer tradizionali;
- a parità di complessità dell'elaborazione, garantire delle performance di esecuzione superiori.

Nonostante nel campo dell'*high performance computing* tradizionale si siano compiuti (e si continuino a compiere) progressi incoraggianti[10], il calcolo tradizionale presenta delle limitazioni tecnologicamente insuperabili[11].

Infatti, alcuni problemi matematici risultano intrattabili dagli elaboratori classici per diverse ragioni:

- non è possibile processare contemporaneamente tutti i dati necessari per l'esecuzione (*space complexity*); ad esempio, la rappresentazione delle possibili configurazioni energetiche degli atomi[12] di una molecola di caffeina, che sono in numero di 10^{48}, non risulta affrontabile con calcolatori tradizionali mentre richiede 160 qubit di un calcolatore quantistico;
- il tempo richiesto dall'esecuzione è irragionevolmente lungo o comunque non compatibile con le esigenze operative (*time complexity*); ad esempio, la scomposizione in fattori primi di un numero naturale che presenta un numero sufficientemente grande di cifre è un'operazione che richiederebbe anche centinaia di anni di calcolo pur impiegando la maggiore capacità computazionale tradizionale esistente;
- la precisione della soluzione calcolata non si dimostra soddisfacente (*inaccuracy*): esistono classi di problemi, come quelli di ottimizzazione, che ammettono più di una soluzione valida (ad

[9] In teoria della complessità computazionale si definisce intrattabile un problema matematico per il quale non esiste un algoritmo "efficiente" (con complessità polinomiale) in grado di risolverlo.

[10] L'High Performance Computing è quella tecnologia in grado di fornire delle prestazioni molto elevate ricorrendo tipicamente al calcolo parallelo.

[11] Il meccanismo alla base del funzionamento dei processori tradizionali è basato su semiconduttori (transistor) che, permettendo o meno il passaggio di corrente, consentono l'applicazione della logica booleana, alla base dell'attuale computazione classica. Il numero di queste componenti all'interno dei microchip (dell'ordine dei miliardi) è direttamente proporzionale alla potenza del processore stesso. Nel corso degli anni la microelettronica è riuscita a diminuire progressivamente le dimensioni di questi oggetti consentendo la corrispondente crescita della potenza di calcolo. Tuttavia, il processo di miniaturizzazione dei transistor sembra trovare un limite proprio negli effetti quantistici di cui risentono alle dimensioni prossime al nanometro.

[12] La singola molecola di caffeina $C_8H_{10}N_4O_2$ è costituita da 24 atomi ciascuno dei quali presenta differenti possibili configurazioni di elettroni nei livelli orbitali disponibili (10^{48}). Un sistema a 160 qubit è in grado di rappresentare 2^{160} possibili configurazioni.

esempio, massimizzare l'uso dello spazio all'interno di una stiva di un aereo adibita al trasporto bagagli). Tuttavia, se in alcuni casi è facile trovare soluzioni subottimali (*local best*), potrebbe risultare estremamente difficile ricercare la miglior soluzione in assoluto (*global best*), specie in presenza di vincoli che complicano la formulazione del problema.

Tra i vantaggi offerti dalla computazione quantistica potrebbe assumere particolare rilievo anche quello legato alla diminuzione dell'impatto ambientale. Da una parte, i quantum computer potrebbero essere sfruttati proprio per analizzare dati, simulare comportamenti (materiali che assorbano carbonio, comportamento catalizzatori) e realizzare modelli per favorire l'analisi e l'individuazione di soluzioni (ottimizzazione della logistica o della distribuzione energetica) per limitare o contrastare gli effetti del cambiamento climatico[13]. Dall'altra il consumo energetico di questi dispositivi (il cui accesso è destinato probabilmente a configurarsi come servizio in cloud) potrebbe essere limitato[14] soprattutto se paragonato all'utilizzo energivoro dei sistemi di High Performance Computing.

3.2.1 L'hardware quantistico

Le due principali tecnologie emergenti di elaborazione quantistica sfruttano due paradigmi di calcolo molto differenti[15]:

1. "*gate-based*" (anche detti *universal* quantum computer): si tratta di una generalizzazione quantistica del tradizionale modello a porte logiche impiegato negli elaboratori classici in cui vengono manipolate e sfruttate le proprietà dei singoli *qubit* attraverso impulsi controllati, campi magnetici, dispositivi ottici o altri meccanismi di controllo;
2. "*adiabatic* quantum *computing*" (anche detti *quantum annealer*): sulla base di un teorema noto in meccanica quantistica (teorema adiabatico) vengono manipolati sistemi di *qubit* controllandone l'evoluzione dinamica, mediante speciali dispositivi (*annealer)*. Il sistema viene preparato in uno stato iniziale e poi fatto evolvere lentamente verso lo stato che rappresenta la soluzione di problemi di individuazione di massimo e minimo (stato ad energia minima).

3.2.1.1 Quantum computer "*gate-based*"

I quantum computer *gate-based* sono basati sulla manipolazione, attraverso una serie finita di "*gates*", di singoli *qubit*. Gli algoritmi sono realizzati tramite una serie di *gate* che formano dei cosiddetti "circuiti".

[13] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/quantum-computing-climate-change-2023.pdf

[14] Premesso che i computer quantistici non sembrano destinati a sostituire quelli tradizionali e il confronto sul rispettivo consumo energetico potrebbe non avere particolare valore, la stima di tale consumo risulta al momento particolarmente complessa sia perché la tecnologia definitiva non è consolidata (ad esempio non tutti i *qubit* richiedono un energivoro sistema di criogenia) sia perché risulta difficile individuare indicatori corretti per valutarne l'impatto. Si rimanda a un progetto (https://quantum-energy-initiative.org/) che mira ad affrontare scientificamente il costo ambientale dell'intero panorama delle tecnologie quantistiche.

[15] Esistono anche dei dispositivi denominati "quantum simulators" che sono progettati per simulare sistemi fisici specifici e ne consentono il controllo per studiare sperimentalmente il comportamento di alcuni problemi fisici di difficile soluzione. Il loro utilizzo, di grande interesse ad esempio in fisica, chimica e farmaceutica, esula dal perimetro del presente resoconto.

Per quanto concerne i tipi di hardware disponibili, ovvero la tecnologia alla base della realizzazione fisica dei *qubit* e la modalità delle loro interazioni, è opportuno premettere che non esiste ancora una tecnologia dominante. La situazione odierna è persino più complessa rispetto a quella che i computer tradizionali hanno vissuto tra gli anni '50 e '60 dello scorso secolo, quando i transistor non si erano ancora imposti sulle valvole termoioniche quale standard costruttivo prevalente. Infatti, esistono molteplici tecniche di realizzazione, con differenti aspetti a favore o di svantaggio, basati su differenti proprietà fisiche quantistiche.

Sulla base dei diversi fenomeni fisici utilizzati, si contano almeno sette differenti approcci per la realizzazione dei *qubit* (vedi box "Tecnologia dei quantum computer: fisica dei *qubit*").

Tecnologia dei quantum computer: fisica dei *qubit*

I differenti approcci per realizzare fisicamente un *qubit* sono:

- *Supercondutive*: grazie alle proprietà dei materiali superconduttori, i quali al di sotto di una temperatura critica conducono elettricità con zero resistenza, è possibile realizzare sistemi in grado di mostrare comportamenti quantistici a livello macroscopico che possono essere manipolati e assemblati in scala. Tuttavia, dispositivi simili per poter operare in modo coerente richiedono ambienti fisicamente isolati e con temperature estremamente basse (< 20 millesimi di grado Kelvin) ottenibili solamente attraverso l'impiego di sofisticati criostati. La tecnologia risulta essere una delle più mature sulla quale hanno investito diversi grandi player di mercato (IBM, D-Wave, Google, Rigetti Computing e IQM).
- *Ion Traps*: i *qubit* sono ottenuti con delle speciali trappole elettromagnetiche per ioni (i.e. atomi carichi positivamente o negativamente). Tali dispositivi, pur risultando almeno di due ordini di grandezza più stabili in termini di tempi di coerenza, sono molto più difficilmente scalabili e nettamente più lenti nell'eseguire i calcoli rispetto ai *qubit* realizzati con superconduttori. Inoltre, sebbene le temperature a cui questi dispositivi riescono a garantire un tempo di coerenza dei qubit sufficiente per la computazione sia maggiore rispetto a quella richiesta dai computer quantistici basati sui qubit a superconduttori, la realizzazione pratica di tali *qubit* richiede l'utilizzo di particolari tecniche di raffreddamento (*laser cooling*) che risultano essere particolarmente energivore. I principali player di mercato in questo segmento sono il consorzio Quantinuum, nato dall'unione del grande gruppo industriale Honeywell e la start up Cambridge Quantum Computing, IonQ e Alpine QT.
- *Neutral Atom*: è una tecnologia simile alle Ion Traps che, invece di intrappolare ioni, confina degli atomi privi di carica – tipicamente in uno stato gassoso – all'interno di camere Ultra-High Vacuum (HUV, con pressioni $\sim 10^{-7}$ Pa). Ciò rende più facilmente scalabili i dispositivi così realizzati, ma, oltre a permanere i problemi di lentezza nei calcoli, si aggiunge la complessità di manipolare i *qubit* ottenuti in questo modo, rendendo più semplice impiegare questi dispositivi come elaboratori analogici, anziché digitali, limitandone di fatto l'impiego a specifiche classi di problemi, in particolare nell'ambito delle simulazioni. I principali player di mercato in questo segmento sono QuEra, Pasqal, Atom Computing e ColdQuanta.
- *Photonic*: in questo caso, i *qubit* corrispondono a dei fotoni che viaggiano lungo circuiti realizzati con comune fibra ottica. Si tratta di una tecnologia estremamente affidabile in termini di coerenza del calcolo, dal momento che le modalità di schermatura del canale in cui quanti di luce interagiscono sono simili a quelle impiegate per proteggere gli impulsi di corrente per la trasmissione dati ed è possibile implementarle a temperatura ambiente (eccezion fatta per i sistemi di rilevazione dei

fotoni che lavorano a una temperatura di ~4K). Tuttavia, risulta particolarmente complesso, rispetto alle altre tecnologie, manipolare fotoni in modo da ottenere dei gate logici operabili in conformità a quanto prevede la teoria dell'informazione quantistica. I principali player di mercato in questo segmento sono PsiQuantum, Xanadu, Quandela e QuiX.

- *Nitrogenvacancy*: prendendo spunto dalle impurità dei diamanti naturali, è possibile realizzare diamanti sintetici in cui si rimpiazzano – nella struttura cristallina – due atomi di carbonio con un atomo di azoto e una lacuna (o cavità reticolare). Tale atomo di azoto (*nitrogen*) funge da *qubit* all'interno della lacuna (*vacancy*) e il suo funzionamento non richiede alcun tipo di prerequisito ambientale. Tuttavia, sistemi di questo tipo non sono pensati per essere scalabili e sono infatti destinati a un potenziale mercato di nicchia on-premise sul quale ha investito la maggiore start up del segmento Quantum Brilliance. Questi dispositivi, di dimensioni limitate ma con un numero ridotto di qubit, possono essere utilizzati per simulazioni e sperimentazioni iniziali di algoritmi quantistici al fine di stimare le risorse di calcolo necessarie per una loro implementazione su larga scala.
- *Spin-based*: i *qubit* corrispondono a elettroni confinati in comuni cavità realizzate con semiconduttori (ad es. il silicio) e i loro stati allo spin (una particolare forma di momento angolare) che l'elettrone può essere indotto ad assumere. La tecnologia non è dissimile a quella impiegata per realizzare i cosiddetti *quantum dots* impiegati nella TV Q-LED già in commercio – pertanto, facilmente scalabile – e, per funzionare in modo coerente, richiederebbe temperature da 1 a 4 Kelvin. Ancorché si tratti di una soluzione prototipale la cui realizzazione ingegneristica rimane da convalidare fattivamente, molti centri di ricerca in tutto il mondo e la stessa Intel sembrano essersi recentemente indirizzati a puntare su questa tecnologia.
- *Topological*: l'idea è quella di costruire porte logiche quantistiche utilizzando i percorsi intrecciati (*braids*) su cui è possibile indirizzare quasi-particelle (sistemi di particelle che si comportano come una unica entità) come gli anioni. A oggi, si tratterebbe dell'unica soluzione senza potenziali controindicazioni. Tuttavia, la tecnologia è ancora estremamente sperimentale e non esistono prove concrete di una sua effettiva realizzabilità. Ciononostante, molte aziende del comparto tecnologico, tra cui Microsoft, stanno investendo molto su di essa.

Sono presenti, tuttavia, caratteristiche comuni a tutte le realizzazioni: la possibilità di inizializzare lo stato di un definito set di *qubit*, di manipolare uno o più di essi tramite dei *gates* che consentano una trasformazione lineare dei loro stati (così come sono le leggi della meccanica quantistica) e, infine, di sottoporli a misurazione dopo l'applicazione dei circuiti previsti dallo specifico algoritmo.

È fondamentale, inoltre, che questi processi avvengano mantenendo la coerenza del sistema fisico e riducendo quanto più possibile gli errori. Ogni elemento che interferisce con i *qubit* (altre particelle, calore, rumore) può rappresentare una "misura" dello stesso. In questo senso si dice che i *qubit* sono "rumorosi", ovvero sono soggetti alla perdita delle loro proprietà quantistiche, come la sovrapposizione o l'*entanglement*. Per identificare i possibili errori vengono utilizzati sistemi di *qubit* dedicati: con il set di *qubit* fisici, contribuiscono alla creazione di *qubit* "logici", con una ragionevole correzione dell'errore[16]. È chiaro che questo è uno degli elementi più complessi di cui tener conto

[16] Il numero dei *qubit* fisici richiesti per la realizzazione di un *qubit* logico dipende dal tipo di algoritmo, dal tipo di errore cui gli specifici *qubit* sono soggetti e dalla loro connessione (gli elementi fisici che consentono di metterne in collegamento uno o più).

per la scalabilità di questi elaboratori e costituisce una particolare area di studio a sé stante che prevede nozioni di elettronica, connettività, criogenia, ecc.

3.2.1.2 Adiabatic quantum computer

I quantum *annealer* sono generalmente ritenuti meno versatili degli *universal* quantum computer in quanto il loro utilizzo è principalmente dedicato alla soluzione di problemi di ottimizzazione mentre il modello a porte logiche si presta allo sviluppo di un più generico set di algoritmi.

Il principio di funzionamento di questi dispositivi è basato sulla previsione della meccanica quantistica secondo cui un sistema, se fatto evolvere lentamente, tende a configurarsi in uno stato energetico minimo.

Allo stato attuale gli *annealer* risultano estremamente più efficaci rispetto ai computer *gate-based* nel risolvere la particolare classe di problemi cui sono dedicati.

3.2.2 Un nuovo paradigma di calcolo

Un primo vantaggio di lavorare con *qubit* configurati in sovrapposizione di stati è che lo spazio della computazione, e conseguentemente il numero di operazioni effettuabili, cresce esponenzialmente al crescere del loro numero, mentre nel mondo classico tale rapporto si mantiene costante. Inoltre, l'*entanglement* quantistico rende possibili operazioni su più *qubit* permettendo la scrittura di algoritmi di calcolo che ne sfruttino le dipendenze, senza necessità che siano contigui nel processore e – in linea teorica – indipendentemente dalla distanza effettiva che li separa.

Rispetto alla computazione tradizionale i tratti distintivi di quella quantistica sono:

- il diverso approccio alla risoluzione dei problemi, che, invece di essere di natura deterministica, è di natura probabilistica;
- l'attuale grado di affidabilità dei dispositivi, ancora piuttosto acerbo quando paragonato all'ottima tolleranza agli errori che i computer classici hanno raggiunto col tempo;
- la mancanza di uno standard ingegneristico predominante per la costruzione dell'hardware, ossia l'equivalente di quello che è il transistor nel mondo classico.

È importante osservare che, anche quando la tecnologia sottostante sia matura e completamente stabile (*fault tolerant*), il quantum *computing* non si candida a rimpiazzare i comuni elaboratori. Il quantum computer (QC) va pensato come un coprocessore estremamente potente da impiegare per risolvere specifiche classi di problemi che oggi risultano – del tutto o in parte – non affrontabili.

Sono noti più di sessanta algoritmi quantistici[17] prodotti negli ultimi 25 anni.

Le principali classi di applicazione sono le seguenti:

[17] Per una panoramica completa e aggiornata di tutti gli algoritmi si rimanda al sito https://quantumalgorithmzoo.org/ dove vengono riportati dettagli sulla tecnologia, dove poterli applicare e i vantaggi in termini di velocità di ciascuno di essi.

- *oracle function-based*: sono compresi principalmente algoritmi di ricerca e conteggio tra cui il più noto è l'algoritmo proposto da Grover[18] e la sua generalizzazione[19] (QAE – "Quantum Amplitude Estimation") che permette il conteggio approssimato del numero di oggetti che soddisfano determinate condizioni all'interno di un set. Si trovano frequentemente come sottoproblemi di vari casi d'uso in ambito finanziario, come la stima delle proprietà statistiche di un campione utilizzata nei metodi Monte Carlo (cfr. 6.1.1.2);
- simulazioni di fisica quantistica e biologia: algoritmi che consentono simulazioni di interazioni tra atomi nelle molecole, utili per lo studio della fisica dei materiali e della biologia molecolare (ad esempio finalizzata alla ricerca di nuovi materiali o farmaci);
- ottimizzazione: algoritmi che ricercano la migliore soluzione di problemi particolarmente complessi come quello del "commesso viaggiatore"[20]; sono impiegati in una grande varietà di scenari (trasporti, logistica, distribuzione energia elettrica, finanza o ambiente); nei quantum *annealer* è possibile utilizzare una classe di particolari algoritmi variazionali[21] che consentono di individuare soluzioni approssimate di diverse classi di problemi di ottimizzazione. (QAOA – *Quantum Approximate Optimization Algorithms*);
- problemi matematici classici noti per essere computazionalmente intrattabili: problemi per i quali non esiste un algoritmo classico efficiente (ovvero con tempi di risoluzione polinomiali[22]) come la fattorizzazione degli interi o il calcolo del logaritmo discreto;
- Quantum *Machine Learning* (cfr. box sottostante): insieme di algoritmi di classificazione e apprendimento che, in determinate condizioni, potrebbero risultare più efficienti dei corrispondenti algoritmi classici attualmente utilizzati.

Quantum Machine Learning (QML)

Il *machine learning* rappresenta quel ramo dell'intelligenza artificiale che studia le correlazioni tra i dati, e, tramite l'applicazione di algoritmi, crea modelli della realtà. In particolare, un software "apprende" da una data esperienza se la sua capacità di eseguire una serie di compiti migliora attraverso l'acquisizione e l'analisi

[18] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, ser. STOC '96, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219, ISBN: 0897917855. https://doi.org/10.1145/237814. 237866

[19] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," AMS Contemporary Mathematics Series, vol. 305, 2000.

[20] Con questo termine ci riferisce a una classe di problemi di teoria dei grafi la cui più tipica rappresentazione è trovare il tragitto di minima percorrenza che un commesso viaggiatore debba seguire per visitare un certo numero di città, con date distanze tra loro e fare rientro a casa.

[21] L'idea di base di un algoritmo variazionale è introdurre soluzioni a un problema in forma parametrica. Questi parametri vengono modificati in una serie di iterazioni successive in modo da raggiungere, attraverso varie tecniche, il minimo della "funzione obiettivo", ovvero la soluzione di un dato problema di ottimizzazione. La caratteristica principale di un algoritmo variazionale è l'utilizzo di risorse computazionali ibride finalizzate all'ottenimento di una soluzione approssimata al problema. La componente quantistica è finalizzata alla misura dello stato di un circuito parametrico, mentre la componente classica minimizza il valore atteso.

[22] Per un problema di dimensione n il tempo o il numero dei passi necessari a trovare la soluzione è una funzione polinomiale di n.

dei dati derivanti da quell'esperienza[23]. Gli algoritmi vengono, quindi, "addestrati" in modo iterativo per essere utilizzati in diversi contesti: effettuare previsioni, identificare correlazioni, interpretare differenti linguaggi e tradurli.

Dal momento che questo tipo di processo richiede sia elevate risorse computazionali, sia l'elaborazione di un ingente quantità di dati per l'apprendimento, è prevedibile che la disponibilità di elaboratori quantistici possa fornire rilevanti vantaggi per integrare, migliorare o rendere più efficienti i modelli di *machine learning* tradizionali nonché svilupparne completamente nuovi basati sul diverso paradigma di calcolo.

L'integrazione di tecnologie quantistiche nel *machine learning*, può tradursi[24] sia nell'uso di dati provenienti da fonti quantistiche (ad esempio dai sensori quantistici) nell'elaborazione classica o quantistica, sia nell'uso di algoritmi quantistici per l'elaborazione di dati classici. Quest'ultimo scenario risulta al momento quello su cui si concentrano la maggior parte degli studi[25].

Si segnalano, a titolo di esempio, due ambiti di ricerca:

- algoritmi che risolvono problemi di ottimizzazione che, in linea di principio, potrebbero migliorare gli attuali meccanismi di apprendimento (al momento si stima un miglioramento di tipo quadratico o polinomiale);
- la possibilità di individuare correlazioni tra le variabili per dividerle in classi: risultati recenti mostrano come, ad esempio, alcuni parametri per il clustering[26] dei dati possano essere stimati con maggiore efficienza utilizzando algoritmi quantistici.

Un esempio riguarda uno dei metodi tradizionali per i problemi di classificazione, SVM (*Support Vector Machine*), il cui obiettivo è riuscire a identificare il confine migliore che separi diverse classi di dati. Il confine migliore è quello che massimizza il margine, ovvero la distanza tra il confine e i punti più vicini di ciascuna classe. Questo calcolo è più agevole quando i dati sono linearmente separabili. Per gestire situazioni dove la separazione non è lineare, l'SVM utilizza una tecnica chiamata "*kernel trick*", che mappa i dati in uno spazio a dimensioni superiori, dove la separazione può diventare lineare. In sostanza, il *kernel* consente di trattare i dati in uno spazio di variabili espanso, semplificando la ricerca del confine ottimale. Questo metodo di mappatura ha dei limiti nel momento in cui lo spazio diventa molto esteso. L'applicazione di metodi quantistici renderebbe possibile la ricerca di soluzioni a problemi di ottimo a dimensionalità altrimenti precluse a metodi classici.

[23] Mitchell, Tom M. *Machine learning*. Vol. 1. , bk. 9. : McGraw-hill New York, 1997.

[24] "An Introduction to Quantum Machine Learning for Engineers" – Osvaldo Simeone - https://arxiv.org/abs/2205.09510

[25] Tra gli altri: Implementation of Quantum Support Vector Machine Algorithm Using a Benchmarking Dataset: https://inspirehep.net/files/33c812bc465883c2210ab4c4c7cd8a42 e Supervised learning with quantum enhanced feature spaces: https://arxiv.org/pdf/1804.11326.pdf

[26] Un processo importante di ML è individuare pattern e relazioni in dati non classificati. A tale scopo si usano tecniche di *clustering* che consentano di identificare gruppi omogenei all'interno di un insieme di dati. Uno di questi algoritmi di *clustering* (K-means) funziona con l'obiettivo di minimizzare la varianza all'interno di ciascun cluster. La versione quantistica consentirebbe un vantaggio esponenziale in questo calcolo.

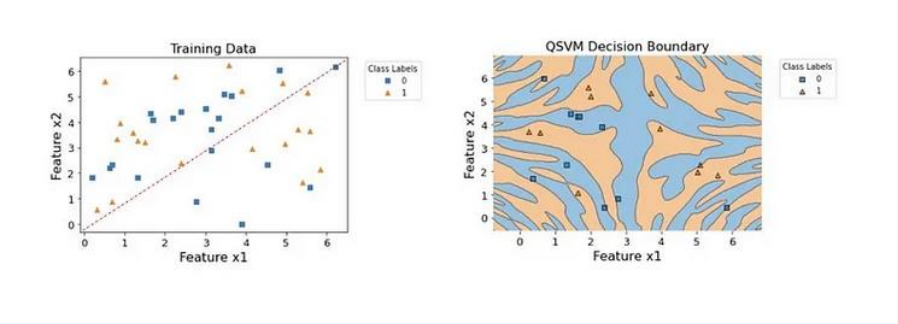


Figura 2 – Esempio semplificato di mappatura bidimensionale di due classi di dati (quadrati e triangoli) utilizzando un algoritmo quantistico[27]

Alla base del vantaggio computazionale offerto da queste varianti quantistiche degli algoritmi, rispetto ai corrispondenti classici, ci sono spesso implementazioni quantistiche di operazioni di calcolo di base (trasformata di Fourier, moltiplicazioni e inversioni di matrici) che risultano molto più efficienti delle corrispondenti classiche[28].

3.3 Quantum *Programming*

Un sistema di computazione quantistica è caratterizzato dall'integrazione di più livelli come descritto nella Figura 3.

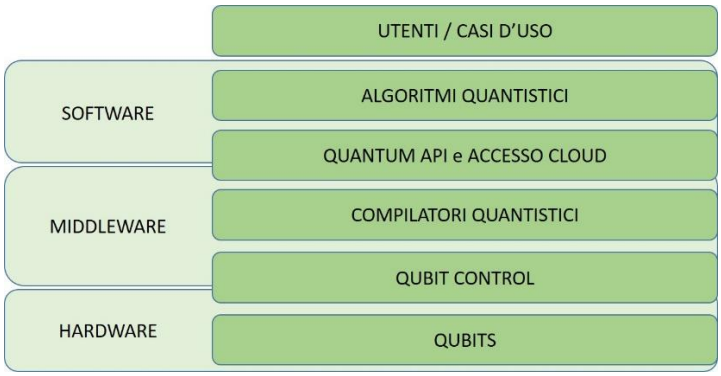


Figura 3 - Quantum computing stack - Strategic Research and Industry Agenda[29]

I *qubit* sono integrati in circuiti che ne prevedono la manipolazione, gli elementi di connessione e controllo. Questi sistemi sono accessibili tramite del software di base che consente di compilare i programmi scritti dagli utenti e inseriti tramite l'accesso alle risorse disponibili solitamente in cloud.

La programmazione quantistica richiede, naturalmente, un approccio diverso rispetto alla programmazione classica. Nonostante sia opportuno avere conoscenze specifiche per sfruttare

[27] https://medium.com/be-tech-with-santander/what-is-quantum-machine-learning-qml-1960c83425f4, il relativo codice è disponibile liberamente: https://github.com/jjprietotorres/QuantumML/tree/master

[28] Uno degli algoritmi quantistici più noti è quello relativo alla fattorizzazione dei numeri interi (Schor) che sfrutta un'implementazione quantistica della trasformata di Fourier (QFT) che permette, in questo caso, di risolvere in tempo polinomiale un problema che "classicamente" risulterebbe intrattabile.

[29] https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf

concetti come sovrapposizione, *entanglement* e misurazione quantistica, si assiste allo sviluppo di *framework* software sempre più accessibili e semplificati.

3.3.1 Approccio alla programmazione

Gli step per la realizzazione di programmi da utilizzare nei quantum computer possono essere sintetizzati come segue:

- definizione del problema;
- scelta dell'algoritmo più conveniente per la sua soluzione;
- scelta del tipo di programmazione (cfr. paragrafo 3.3.2);
- scrittura del codice;
- esecuzione del codice in simulatori o nell'hardware quantistico;
- interpretazione del risultato.

L'approccio tradizionale alla programmazione di un computer quantistico prevede la presenza di un computer classico che non solo piloti un processore quantistico, ma ne elabori anche le soluzioni per consentire l'iterazione di sotto-problemi in fasi successive.

L'architettura è simile a quella utilizzata nei centri di super calcolo:

- si predispongono in un computer classico, in modalità *batch* (modalità pianificata), le attività che devono essere eseguite (*jobs*);
- i *jobs* vengono inviati al calcolatore (quantum computer) tipicamente attraverso un fornitore di servizi (Quantum Cloud Provider);
- si interpretano i risultati su un computer classico (esempio di Figura 4).

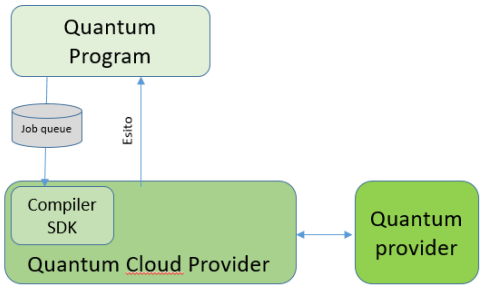


Figura 4 – Approccio alla programmazione di un computer quantistico[30]

Dal momento che l'accesso all'hardware reale, tipicamente via cloud, è condiviso da migliaia di utenti ogni giorno, ciascun provider di tecnologia stabilisce normalmente un limite massimo di esecuzioni giornaliere o mensili per ciascun utente.

[30] Liberamente tratto da "Quantum Computing Toolkit From Nuts and Bolts to Sack of Tools" - Himanshu Sahu, Hari Prabhat Gupta https://arxiv.org/pdf/2302.08884.pdf

Anche per questo motivo, per la prototipizzazione o l'ingegnerizzazione del software risulta preferibile l'utilizzo di un simulatore di hardware quantistico su computer classici, dal momento che consente di stimare i risultati attesi da un dispositivo reale e di ottimizzare l'esecuzione senza dover "consumare" accessi all'hardware quantistico. L'utilizzo di quest'ultimo è così relegato tipicamente alle fasi finali in cui si intende verificare il funzionamento dell'applicativo.

L'utilizzo dei NISQ, i dispositivi oggi disponibili con ridotti *qubit* e soggetti a rumore ed errori, si basa sull'esecuzione ripetuta dell'algoritmo che consente di effettuare una media sul risultato ottenuto in modo da aumentare la sua precisione.

3.3.2 Quantum *programming languages*

3.3.2.1 Programmazione tramite circuiti quantistici

La programmazione basata sulla costruzione di "circuiti quantistici" prevede l'introduzione di una sequenza di operazioni chiamate porte quantistiche (*gates*), nella pratica riconducibili a operazioni matematiche. Tali operazioni, applicate ai singoli *qubit*, cambiano gli stati quantici dei *qubit* e le loro relazioni, consentendo, attraverso la loro manipolazione, di risolvere determinati problemi.

Nella programmazione di un quantum computer, le misurazioni vengono generalmente eseguite alla fine del circuito quantistico, dopo che sono stati applicati tutti i gate desiderati. Durante l'esecuzione delle operazioni quantistiche, il *qubit* può trovarsi in uno stato di sovrapposizione, ma la misurazione finale determina il risultato finale in termini di bit classici (0 o 1).

Ne consegue che il ciclo di sviluppo di un programma per quantum computer segue il classico processo *Build-Compile-Run-Analyze*, ma con le peculiarità del quantum *computing*, fino a ora evidenziate.

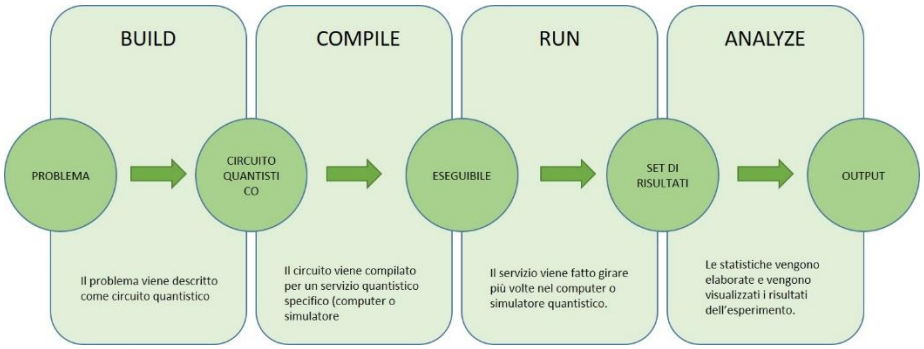


Figura 5 - *The quantum development life cycle*[31]

Vantaggi:

- interpretazione "geometrica" chiara di come i *qubit* evolvono durante l'esecuzione di un algoritmo;
- controllo su ciascuna operazione quantistica applicata: è possibile progettare circuiti specifici per soddisfare le esigenze dei diversi algoritmi;
- costruzione graduale del circuito (le porte quantistiche vengono aggiunte una alla volta, e l'evoluzione dello stato può essere analizzata a ogni passo);

[31] Tratto da https://arxiv.org/pdf/2302.08884.pdf

- ottimizzazione delle prestazioni dello specifico algoritmo grazie a maggiore flessibilità.

Svantaggi:

- necessità di una buona conoscenza della teoria quantistica e familiarità con l'algebra lineare per la comprensione delle interazioni.

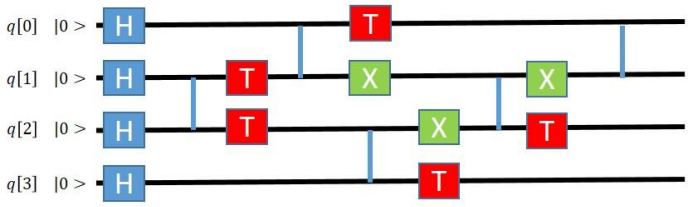


Figura 6 - Esempio di come appaia graficamente un circuito quantistico: all'inizio i quattro *qubit* sono inizializzati nello stato |0> , in seguito vi sono applicati diversi gates (ad esempio il gate X è l'equivalente quantistico dell'operatore classico NOT e trasforma lo stato del *qubit* da |0> a |1> e viceversa).[32]

3.3.2.2 Programmazione tramite linguaggi di alto livello o Software Development Kit (SDK)

Per semplificare la programmazione dei computer quantistici sono state introdotte negli ultimi anni librerie che permettono di fornire un buon livello di astrazione.

I *framework* per il quantum *computing* tipicamente si occupano di tre ambiti:

- interfacciare l'hardware quantistico, fornito dal produttore del *framework* o da altri[33];
- simulare gli eseguibili su hardware classico;
- semplificare lo sviluppo di procedure ottimizzate per il quantum *computing*.

Python è uno dei linguaggi di programmazione più utilizzati, in quanto popolare e versatile, facile da imparare e equipaggiato con una vasta gamma di librerie e strumenti disponibili per la programmazione quantistica.

Vantaggi:

- alto grado di astrazione che consente la programmazione ai non esperti di fisica quantistica;
- possibilità di riutilizzare in diversi contesti funzioni quantistiche generiche;
- possibilità di integrare funzionalità classiche, consentendo una maggiore interazione.

Svantaggi:

- mancanza di controllo dettagliato sul circuito quantistico e della relativa flessibilità;
- meno efficienza nell'implementazione rispetto a circuiti ottimizzati manualmente da esperti.

Gli SDK possono essere offerti tramite licenze proprietarie o open source, in questo resoconto saranno brevemente descritti (cfr. 4.5.3) solo questi ultimi, in quanto più utilizzati e supportati da community più vaste che li evolvono nel tempo.

[32] Tratto da https://www.redhotcyber.com/post/i-circuiti-quantistici-terza-lezione/

[33] Normalmente una stessa SDK è in grado di interfacciarsi ad hardware differenti (cfr. 4.5.3).

3.4 Crittografia quantistica

3.4.1 Le minacce alla crittografia tradizionale

I meccanismi crittografici comunemente utilizzati per garantire la riservatezza e l'integrità delle comunicazioni prevedono l'uso combinato di due tipi di crittografia: asimmetrica o "a chiave pubblica" e simmetrica o "a chiave privata". In particolare la crittografia asimmetrica è generalmente utilizzata per lo scambio iniziale di chiavi che vengono poi utilizzate per cifrare i dati tramite crittografia simmetrica.

L'interesse a individuare ulteriori strategie per la crittografia, differenti da quelle in uso, nasce con la scoperta nel 1994, da parte dell'informatico statunitense Peter Shor, di un algoritmo capace di risolvere in tempi ragionevoli il problema della fattorizzazione degli interi la cui complessità è alla base degli attuali meccanismi di crittografia a chiave asimmetrica.

Per quanto riguarda la crittografia simmetrica, gli algoritmi esistenti, e in particolare quello proposto da Lov Grover nel 1966, non costituiscono un particolare rischio per una sua violazione: il vantaggio risultante dalla computazione quantistica potrebbe essere facilmente arginato utilizzando una chiave più lunga[34].

Ne consegue che le minacce provenienti dalla disponibilità di elaborazione quantistica sono rivolte alla robustezza della componente asimmetrica nell'utilizzo della crittografia a chiave pubblica utilizzato per lo scambio delle chiavi. Le infrastrutture IT e le applicazioni fanno affidamento su soluzioni (come RSA – Rivest, Shamir, Adleman o ECC – *Elliptic Curve Cryptography*) basate su questa crittografia per garantire la confidenzialità e l'integrità dei dati sia che essi transitino tra controparti, sia che siano conservati all'interno dei *data center*.

Algoritmo crittografico	Scopo	Impatto disponibilità di QC
AES-256	Cifratura simmetrica	Sicuro
SHA-256	Funzioni di hash[35]	Sicuro
RSA	Scambio di chiavi, firma	Violato
ECC	Scambio di chiavi, firma	Violato
DSA	Scambio di chiavi, firma	Violato

Tabella 1 - Sicurezza dei principali algoritmi utilizzati in crittografia (fonte NIST[36])

[34] L'algoritmo di Grover consente di trovare un record in un database non ordinato in $\sqrt{n}$ passaggi (il miglior algoritmo classico ne richiede $n/2$). Tale algoritmo ridurrebbe la sicurezza della crittografia a chiave simmetrica di un fattore radice e non rappresenterebbe, al momento, una seria minaccia per la crittografia simmetrica.

[35] Una funzione hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita, generalmente utilizzata per verificare l'integrità di un messaggio.

[36] Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms (nist.gov).

Esistono due ambiti di indagine per l'individuazione di soluzioni alternative ai meccanismi di cifratura noti. Il primo è rappresentato dalla crittografia "post-quantum" (PQC), basata sull'impiego di problemi matematici complessi per i quali non esiste un algoritmo quantistico in grado di violarne la sicurezza, che consentirebbe di rendere quantum *safe* lo schema di cifra basato su chiave asimmetrica. Il secondo, Quantum *Key Distribution* (QKD), invece, risolve il problema dello scambio della chiave che interessa la cifratura asimmetrica grazie alla possibilità, offerta dalle proprietà della meccanica quantistica, di garantire uno scambio di chiavi sicure tra due interlocutori. PQC e QKD rappresentano due approcci complementari con un differente livello di maturità il cui utilizzo, anche in combinazione, può essere ipotizzato in differenti scenari.

3.4.2 Post-Quantum *Cryptography*

La crittografia post-quantistica è lo studio di sistemi crittografici, basati su problemi matematici per cui non sono noti algoritmi che rendano più efficiente l'individuazione della soluzione, come per la scomposizione in fattori primi. L'introduzione di questi meccanismi può avvenire sui computer classici utilizzando lo schema già consolidato di crittografia a chiave pubblica e continuerebbe a garantire la confidenzialità anche in presenza di un attaccante che possa utilizzare il calcolo quantistico.

Nel 2016 il NIST, l'ente di standardizzazione statunitense, ha avviato una competizione per individuare alcuni algoritmi di cifratura e per la firma digitale da poter utilizzare come standard e avviare il relativo processo (cfr. 4.2.3). Dopo una accurata selezione, resa più stringente anche dall'attacco a uno degli schemi di firma digitale finalisti[37], sono stati individuati nell'estate 2022 quattro algoritmi, tre per la firma digitale[38] (CRYSTALS-Dilithium, SPHINCS+ e FALCON) e uno per la cifratura (CRYSTALS-Kyber).

Naturalmente, l'obiettivo ultimo della PQC è la sostituzione degli algoritmi attualmente in uso con quelli considerati più sicuri, cercando di rendere la transizione meno onerosa possibile. Tuttavia, l'operazione non risulta così semplice a causa dell'eterogeneità degli algoritmi proposti sino ad ora (ad esempio essi differiscono per lunghezza della chiave richiesta). Inoltre, il loro utilizzo comporta un maggiore costo computazionale che potrebbe rivelarsi troppo oneroso in taluni *use case* dove la frequenza di scambio delle chiavi è alta, oppure in dispositivi con limitate capacità hardware (IoT).

Diversi produttori di software e di tecnologie si stanno concentrando nell'inserire nel loro piano di sviluppo la possibilità di sfruttare tali algoritmi. Va notato, tuttavia, che non ci sono ancora linee guida accettate a livello europeo per l'eventuale adozione di questi standard anche se recentemente è stata emanata una raccomandazione[39] (cfr. 4.2.3) per l'introduzione di una *roadmap* condivisa per la transizione alla crittografia Post-Quantum.

[37] "Breaking Rainbow Takes a Weekend on a Laptop" - https://link.springer.com/chapter/10.1007/978-3-031-15979-4_16

[38] Il NIST ha tuttavia dichiarato l'intenzione di riaprire la competizione per la firma digitale in quanto due dei tre algoritmi sono basati sulla matematica dei reticoli, fattore che rende più fragile la loro robustezza.

[39] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

3.4.3 Quantum *Key Distribution*

È noto dalla teoria dell'informazione che se mittente e destinatario dispongono di una chiave costituita da sequenza di numeri genuinamente casuali abbastanza lunga (idealmente quanto il messaggio stesso), essi sono in grado di scambiarsi un messaggio in modo "incondizionatamente" sicuro[40]. Le difficoltà di questo schema consistono proprio nella costruzione di una chiave random e nella sua distribuzione sicura, possibilità attualmente offerta dagli algoritmi a chiave asimmetrica tramite l'impiego delle funzioni matematiche prima descritte che risultano vulnerabili al nuovo paradigma di calcolo.

Le tecniche relative alla distribuzione quantistica delle chiavi, Quantum *Key Distribution* (QKD), consentono la distribuzione sicura di chiavi *random*, da impiegare nella cifratura simmetrica sfruttando sia le proprietà di sovrapposizione di stati e/o *entanglement* che caratterizzano i sistemi microscopici sia il ruolo di interferenza rappresentato dall'operazione di misura di questi stati fisici.

Le particelle subatomiche più utilizzate in questo ambito sono quelle di cui è composta la luce, ovvero i fotoni. Questi possono venire facilmente emessi e trasmessi attraverso le fibre ottiche su cui si basano le attuali comunicazioni di rete e rilevati attraverso specifici dispositivi. L'informazione viene codificata in particolari proprietà fisiche dei fotoni come la polarizzazione (cfr. 3.1).

Attraverso schemi predefiniti tra due interlocutori Alice e Bob, precedentemente autenticati, che prevedono, ad esempio, la preparazione da parte del mittente e la misura da parte del destinatario degli stati di polarizzazione di fotoni, è possibile fare in modo che questi condividano una stringa di bit random da utilizzare come chiave di cifratura.

I dettagli[41] di come questo possa accadere possono essere approfonditi da varie fonti[122]: in estrema sintesi entrambi utilizzano dei polarizzatori rispettivamente per codificare e decodificare il segnale e ottenere una chiave. Quest'ultima viene estratta dai risultati della misura della polarizzazione di fotoni quando entrambi gli interlocutori utilizzano la medesima base per la preparazione dello stato del fotone (Alice) e la sua misura (Bob). Tali valori sono random, coincidono e sono noti solo a entrambi.

È importante notare come sia la comunicazione della sequenza di basi utilizzate, sia la trasmissione del segnale stesso, possano avvenire in un canale in chiaro: un'eventuale intercettazione verrebbe rilevata grazie al fatto che, come già sottolineato, qualunque tentativo di misurare il segnale ne distruggerebbe le proprietà e sarebbe facilmente riconoscibile. Infatti, il protocollo prevede che Alice e Bob dichiarino pubblicamente una parte statisticamente rilevante dei risultati delle misure effettuate per verificare che coincidano e che il segnale non abbia subito alterazioni.

Nelle realizzazioni pratiche, un sistema QKD prevede, quindi, le seguenti componenti:

[40] La dimostrazione matematica dell'inviolabilità si deve a Claude Shannon nell'articolo "Communication Theory of Secrecy Systems" (1949).

[41] BB84 rappresenta il primo e più utilizzato algoritmo di quantum *key distribution* funzionante, codificato e applicato su piccola scala dai due fisici C. Bennet e G. Brassard nel 1984.

- un generatore di numeri genuinamente casuali, anch'esso ottenibile sfruttando il comportamento aleatorio delle variabili quantistiche (cfr. 3.5) per la produzione di una chiave random;
- dispositivi per l'emissione e la rilevazione di singoli fotoni;
- un collegamento in fibra dedicato alla trasmissione della chiave (quantum *channel*);
- un collegamento[42] per la trasmissione del messaggio cifrato (*classical channel*);
- un protocollo per l'elaborazione della chiave tra le controparti.

La sicurezza della teoria sottostante alla QKD fa leva sulla natura ineludibilmente stocastica del processo di misura nel mondo microscopico ma la possibilità di sfruttare questo comportamento nelle realizzazioni pratiche è legata alla capacità di mantenere inviolate le proprietà delle particelle coinvolte. Di conseguenza, è facile comprendere che gli attuali sistemi di scambio chiavi tramite un canale diretto in fibra ottica abbiano un range limitato dovuto alla dispersione del segnale.

La QKD è dimostrata anche nelle comunicazioni satellitari per ottenere distanze considerevolmente maggiori[43] ma questo tipo di trasmissione richiede investimenti su scala nazionale o sovranazionale.

3.4.3.1 Quantum Communication

L'area della comunicazione quantistica ha per scopo l'individuazione di soluzioni hardware, software e protocolli per elaborare e scambiare informazioni quantistiche attraverso la rete e, in particolare, attraverso i quanti di luce (fotoni) che sono attualmente comunemente utilizzati nelle fibre ottiche e che possono essere trasmessi attraverso l'atmosfera nella comunicazione satellitare.

Lo scambio di informazioni sicure garantito dall'infrastruttura QKD è realizzabile per la trasmissione punto-punto su distanze limitate (attorno ai 100 Km) utilizzando soluzioni già disponibili sul mercato con un alto livello di *technological readiness* (TRL), ma rimangono sfide per quanto riguarda gli aspetti di integrazione e interoperabilità. L'utilizzo dello schema QKD descritto in precedenza diventa più complesso nel momento in cui si affrontano topologie di rete più articolate rispetto a quella "punto-punto". La difficoltà risiede nell'impossibilità di utilizzare apparati di rete intermedi, come ripetitori tradizionali, che, nel manipolare il segnale, interferirebbero con la sovrapposizione di stati (al pari di qualunque interferenza) rendendo inutilizzabile l'applicazione del protocollo.

Si ipotizza l'utilizzo di varie tecnologie, con diversi aspetti di affidabilità, sicurezza e costo[44]. È necessario introdurre elementi di rete completamente nuovi rispetto agli apparati comunemente utilizzati nelle reti tradizionali. La ricerca si sta concentrando su differenti meccanismi per garantire

[42] La trasmissione dei dati relativi alla chiave e al messaggio può avvenire, in linea di principio, utilizzando lo stesso canale ottico ma, per ragioni di interferenza, è preferibile l'uso di un canale dedicato alla distribuzione della chiave. La coesistenza può avvenire utilizzando tecniche di multiplexing di frequenza (WDM), *time sharing* (TDM) oppure isolando fibre dedicate (Space Division Multiplexing). Da notare, inoltre, che sorgente e destinatario necessitano di essere autenticate per garantire la sicurezza della trasmissione: è necessario servirsi di chiavi *pre-shared*, fornite dal costruttore, oppure utilizzare meccanismi di autenticazioni basati sulla post-quantum *cryptography*.

[43] La perdita di fotoni è molto inferiore nella trasmissione satellitare rispetto alle fibre dato che essi viaggiano per lo più nel vuoto è sono condizionati solamente dall'assorbimento atmosferico e lo *scattering* che avvengono nei 10 Km di atmosfera più vicini alla terra.

[44] Per una panoramica si può consultare Quantum Key Distribution: A Networking Perspective di Mehic et al.- https://dl.acm.org/doi/abs/10.1145/3402192

maggiori distanze: *trusted nodes* (nodi in cui l'informazione è processata e ritrasmessa), quantum *repeaters* (basati sulla combinazione di processi di *entanglement*) o l'utilizzo della rete satellitare per coprire grandi distanze.

La prospettiva a lungo termine è quella di riuscire a realizzare una infrastruttura di comunicazione quantistica che consenta la comunicazione a qualunque interlocutore del pianeta sfruttando una combinazione eterogenea di soluzioni per la propagazione del segnale e una moltitudine di operatori dislocati nel territorio internazionale.

3.4.4 Post-Quantum *Cryptography* vs Quantum *Key Distribution*

Gli approcci descritti nei paragrafi precedenti presentano caratteristiche ed elementi di applicabilità differenti come sintetizzato nelle tabelle seguenti. La loro integrazione nell'attuale assetto di sicurezza va valutata in modo complementare.

Post-Quantum *Cryptography* (PQC)	**Quantum *Key Distribution* (QKD)**
Sicurezza legata alla complessità di funzioni matematiche, potenzialmente vulnerabili nel momento in cui si identificassero algoritmi per farlo.	Sicurezza "incondizionata", basata sul comportamento delle particelle a livello subatomico.
Richiede modifiche applicative alle chiamate crittografiche del software.	Richiede dispositivi hardware specializzati, una connessione in fibra ottica dedicata e delle interfacce verso dispositivi o software di cifratura.
Non dipende dal mezzo di trasmissione.	Può essere utilizzata solo tramite fibre ottiche o comunicazioni satellitari.
Costi per l'individuazione e la sostituzione delle chiamate crittografiche dipendenti dal parco applicativo in uso.	Costi elevati per la predisposizione dell'infrastruttura per la trasmissione in fibra e al momento insostenibili per la comunicazione satellitare.
Non dipendente dalla distanza, completamente compatibile con i ripetitori tradizionali.	Distanza di comunicazione per trasmissioni in fibra ottica limitata a circa 100 Km, necessità di ripetitori quantistici, *trusted nodes* o collegamenti satellitari per trasmissioni su più vasta scala.
Alcuni algoritmi richiedono una lunghezza della chiave maggiore.	Lunghezza della chiave di dimensioni standard per il protocollo simmetrico.
Possono essere utilizzati firme digitali o certificati per l'autenticazione.	Per considerare affidabile lo scambio delle chiavi sorgente e destinatario devono essere autenticati tramite crittografia asimmetrica PQC o *preshared keys*.

Tabella 2 - PQC vs QKD (caratteristiche)

Post-Quantum *Cryptography* (PQC)	**Quantum *Key Distribution* (QKD)**
Soluzione general/purposes. Alcuni software commerciali hanno già una *roadmap* di adozione.	Soluzione adatta per casi di utilizzo molto specifici come ad esempio la protezione dei collegamenti tra centri elaborativi in ambito metropolitano.
Sicurezza nel breve/medio periodo.	Sicurezza nel lungo periodo.
Adatta anche agli algoritmi di firma e autenticazione.	Non utilizzabile per la firma digitale.

Tabella 3 - PQC vs QKD (*use case*)

È opportuno sottolineare che esiste un dibattito sull'opportunità di investimento nell'uno o nell'altro scenario. L'NSA, l'agenzia nazionale statunitense per la sicurezza, non raccomanda l'utilizzo della QKD fino a quando non si siano superate alcune limitazioni (necessità di autenticare i nodi e di utilizzo di dispositivi dedicati non disponibili su scala industriale e con un grado di affidabilità non convincente). Anche alcune agenzie europee, come l'ufficio federale per la sicurezza nell'informatica tedesco[45], preferiscono mantenere un approccio conservativo verso questa tecnologia.

Il governo USA spinge, infatti (cfr. 4.3.1.1), all'utilizzo diffuso della crittografia post-quantum che ritiene più conveniente nel rapporto costi benefici. La raccomandazione all'uso di questi ultimi algoritmi ha trovato solo recentemente una ufficializzazione da parte dell'Europa (cfr. 4.3.2.6), mentre Cina e Russia sembrerebbero orientate a individuare algoritmi alternativi a quelli proposti dal NIST.

3.5 Quantum *Random Number Generator*

La generazione efficace di numeri casuali è di massimo rilievo in svariati ambiti scientifici per esempio nell'effettuare simulazioni affidabili e modellazioni statisticamente robuste di sistemi fisici (o econofisici). Anche in informatica, per garantire la sicurezza di una chiave crittografica è necessario garantirne la randomicità. A tale scopo si utilizzano diffusamente i cosiddetti Generatori di Numeri Pseudo-Casuali (PRNGs): da essi dipende l'effettivo successo di tutti i protocolli di cifratura esistenti e la riuscita di simulazioni stocastiche come quelle di tipo Monte Carlo.

Generazione di numeri casuali

L'ottenimento di sequenze di numeri casuali è legato all'utilizzo di sorgenti che siano in grado di generare sequenze di bit ad alta entropia[46]. Questo è possibile utilizzando come sorgente di entropia la misurazione di proprietà fisiche di sistemi che abbiano una evoluzione temporale non deterministica (Figura 7).

Nei calcolatori classici, tuttavia, questa sorgente non è facilmente accessibile e questa funzione è realizzata attraverso programmi per la generazione di sequenze di numeri (denominati, infatti, "pseudo casuali") che elaborano in maniera completamente deterministica valori di input. Pur essendo molto economici, per loro natura questi metodi presentano una intrinseca debolezza che li rende inadatti in molti contesti, in particolare nell'uso di chiavi crittografiche.

[45] https://www.squad-germany.de/en/position-paper-on-quantum-key-distribution/

[46] L'entropia di una sorgente è definita, in teoria dell'informazione (Shannon), come "il valore atteso dell'autoinformazione, ovvero l'informazione media contenuta in ogni messaggio emesso". Trattando una sorgente di entropia come una scatola chiusa che genera valori, si evince come la quantità di entropia che essa genera è proporzionale all'informazione dei bit che emette. Una sorgente che emette bit tutti dello stesso valore ha una entropia pari a 0.

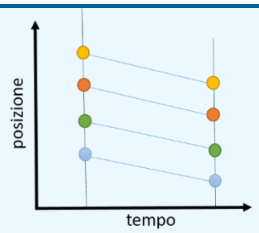


Figura 7 - Evoluzione deterministica

Per migliorare la qualità dei numeri casuali si possono utilizzare dei dispositivi hardware in grado di convertire in segnale digitale alcuni parametri di fenomeni fisici imprevedibili come quelli a evoluzione caotica (Figura 8) che caratterizzano, ad esempio, i moti turbolenti in fluidodinamica o fenomeni metereologici tali per cui piccole variazioni delle condizioni iniziali provochino cambiamenti considerevoli negli output.

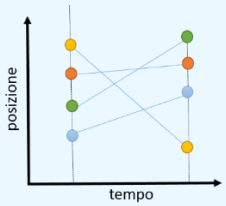


Figura 8 – Evoluzione caotica

Il valore di output di tali meccanismi non può essere utilizzato direttamente come sequenza casuale; sono infatti richieste tecniche per rimuovere la distorsione (*bias*) della sorgente fisica (ovvero la caratteristica per cui la probabilità di osservare un dato *outcome* sia diversa da quella di un altro). Le sorgenti di informazioni casuali (sorgenti di entropia) di questo tipo, inoltre, oltre a non essere molto efficienti, possono essere soggette ad attacchi che tendano ad alterare in modo artificiale i loro parametri ambientali (es. temperatura) in modo da annullare gli effetti non deterministici che sono alla base del loro funzionamento.

I generatori di numeri casuali quantistici (QRNGs), basati sull'indeterminazione intrinseca delle misurazioni quantistiche, rappresentano il modo per ottenere quel parametro di casualità - cosiddetto "random seed" - completamente imprevedibile di cui si ha necessità (Figura 9). Essi rappresentano una sorgente di entropia più affidabile, veloce, e ad alto rendimento rispetto ai generatori classici disponibili.

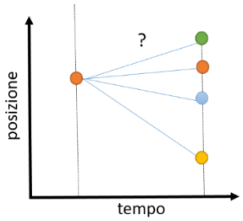


Figura 9 - Evoluzione random

I primi QRNG erano basati sul processo di decadimento radioattivo di alcuni elementi, che sfortunatamente avevano lo svantaggio di emettere radiazioni dannose per la salute, limitandone la diffusione, mentre i più moderni dispositivi si basano sull'utilizzo di fotoni che presentano facilità e basso costo di realizzazione e possono facilmente essere inseriti all'interno di dispositivi pratici. In

particolare si sfruttano processi imprevedibili ed equiprobabili, ad esempio, la trasmissione o riflessione di fotoni su uno specchio semitrasparente. Una sorgente di fotoni (a diodo o a laser) emette fotoni in sovrapposizione di stati (ciascuno di essi ha il 50% di probabilità di venire riflesso e il 50% di venire trasmesso) verso una superficie semitrasparente a valle della quale viene registrato il corrispondente valore tramite due rilevatori posti nella direzione di riflessione e trasmissione.

La sequenza di valori ottenuti, opportunamente tradotta in termini binari e sottoposta a tecniche per massimizzarne l'entropia, può essere utilizzata come base per tutti i processi che richiedano numeri genuinamente casuali.

3.6 Quantum *Sensing*

L'ambito del quantum *sensing* comprende una serie di dispositivi avanzati in grado di rilevare con notevole accuratezza determinati valori di grandezze fisiche sfruttando fenomeni quantistici. In particolare, i sensori quantistici possono essere utilizzati per misurare con una sensibilità elevata campi elettromagnetici, temperatura e pressione e il loro utilizzo è già stato introdotto in differenti campi della ricerca scientifica. Oltre a una maggiore accuratezza, i sensori quantistici forniscono altri vantaggi, come la possibilità di eseguire misure non invasive (utile soprattutto nel campo della diagnostica medica) e la velocità nella misura (praticamente real time).

Il loro funzionamento di base presenta delle analogie con quello sfruttato nella costruzione dei *qubit* per l'elaborazione quantistica. Per esempio[47] alcuni di essi si basano sulla misurazione di proprietà di atomi o ioni confinati nel vuoto e raffreddati a basse temperature, quindi manipolati tramite laser o radiazioni[48] oppure su effetti dell'interazione con singoli fotoni.

I principali dispositivi in commercio sono:

- orologi atomici basati sulla stabilità di oscillazione di atomi come cesio e rubidio;
- magnetometri, gravitometri e termometri;
- sensori chimici per i rilievi ambientali;
- sensori di immagini che utilizzano la proprietà di fotoni e atomi di creare immagini ad alta risoluzione della struttura della materia.

I sensori quantistici presentano vantaggi in molte applicazioni quali: *bio-imaging*, spettroscopia, comunicazione, navigazione, monitoraggio ambientale, monitoraggio infrastrutturale, ispezione geografica, fisica delle alte energie di cui si cita qualche esperienza:

- il progetto Swarm dell'Agenzia Spaziale Europea ha utilizzato[49] dei magnetometri quantistici per creare una mappa dettagliata del campo gravitazionale terrestre;

[47] https://research.aimultiple.com/quantum-sensors/

[48] Per esempio, se esposti ad un campo magnetico, gli atomi e ioni isolati all'interno del sensore subiscono effetti sulla distribuzione dei livelli energetici. Questi possono essere rilevati tramite spettroscopia laser e consentire la misura accurata del campo magnetico stesso.

[49] https://earth.esa.int/eogateway/missions/swarm

- l'esercito USA ha previsto[50] l'utilizzo di sensori quantistici per migliorare i sistemi di navigazione basati su GPS;
- i ricercatori dell'università del Sussex hanno sviluppato[51] un sensore quantistico in grado di intercettare cambiamenti nelle proprietà magnetiche delle cellule tumorali che potrebbe migliorare gli strumenti di diagnostica.

Nonostante il livello di maturità dei dispositivi di quantum *sensing* sia tra i più elevati nell'ambito delle tecnologie quantistiche (cfr. 4.5.1), in ambito bancario non sono note applicazioni specifiche diverse da quelle di monitoraggio dei parametri ambientali per i quali non si intravede, al momento, la necessità di *performance* migliori rispetto a quella assicurata dai rilevatori classici.

[50] https://www.iotworldtoday.com/industry/us-air-force-awards-sandboxaq-quantum-navigation-research-contract
[51] https://www.sussex.ac.uk/broadcast/read/55573

4 “Ecosistema” delle tecnologie quantistiche

4.1 Le competenze quantistiche

La natura dello studio delle tecnologie quantistiche è, inevitabilmente, interdisciplinare e richiede conoscenze approfondite non solo in ambiti scientifici e tecnici (matematica, fisica, informatica e ingegneria), ma, per cogliere le opportunità, comprendere i rischi, affrontare i relativi progetti tali competenze vanno integrate con quelle economiche, sociali e, ad alcuni livelli, geopolitiche. Alcuni analisti[52] stimano che, nel 2025, il 50% dei lavori nell’ambito quantum rimarranno senza candidati a causa della difficoltà a reperire personale con le necessarie competenze nel mercato.

La Commissione europea ha promosso il progetto QTEdu[53] per favorire la consapevolezza e la formazione nell’ambito delle tecnologie quantistiche, che, tra le altre cose, individua un *framework* di competenze[54] (Figura 10 e Figura 11) ritenute strategiche per la loro introduzione nel mondo industriale, stimando anche il tempo necessario per la loro acquisizione.

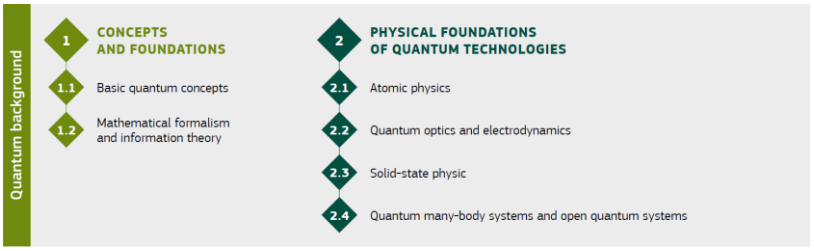


Figura 10 - European Competence Framework for Quantum Technologies – Version 2.0 - Quantum background

[52] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

[53] https://qtedu.eu/

[54] Greinert, F., Müller, R. (2024). European Competence Framework for Quantum Technologies 2.5. Zenodo. https://zenodo.org/records/10976836

Figura 11 - European Competence Framework for Quantum Technologies – Version 2.0 – Core device technologies e QT systems and applications.

Tra i principali centri di ricerca a livello globale vanno considerati il Massachusetts Institute of Technology (MIT)[55] che offre anche l’opportunità di corsi online nella piattaforma MIT Xpro, l’Institute for Quantum Computing dell’università di Waterloo[56] attivo già dal 2002, la Harvard University[57] e la Max Planck Society[58]. Una panoramica dell’offerta accademica italiana è riportata al paragrafo 4.4.3.

Di seguito un elenco di eventi e iniziative che possono essere utili ad ampliare le proprie conoscenze sui risultati più recenti, conoscere le varie strategie e creare una rete di collaborazione:

- il sito web di QTEdu[53] dove sono raccolti riferimenti a risorse e iniziative per la formazione a vari livelli di conoscenza e per vari interlocutori a partire dalla scuola primaria;
- differenti eventi organizzati da IEEE[59] (International Conference on Quantum Software e IEEE Quantum Week);
- il workshop annuale del CINECA[60] (Consorzio Interuniversitario del Nord-Est per il Calcolo Automatico) in collaborazione con l’Università degli Studi di Milano su “High Performance Computing and Quantum Computing”;

55 https://physics.mit.edu/research-areas/quantum-information-science/
56 https://uwaterloo.ca/institute-for-quantum-computing/
57 https://quantum.harvard.edu/
58 https://www.imprs-quantum.mpg.de/
59 https://quantum.ieee.org/
60 https://www.quantumcomputinglab.cineca.it/

- l’Osservatorio del Politecnico di Milano[61] che prevede attività di ricerca, occasioni di confronto e approfondimento destinate agli iscritti e un convegno pubblico di presentazione delle attività di ricerca.

Eventi che prevedono un maggiore coinvolgimento di realtà industriali e commerciali:

- gli appuntamenti, dei quali uno si svolge annualmente in Europa, della società Inside Quantum Technology[62] che si occupa di fornire articoli, aggiornare news e produrre report sulle tecnologie quantistiche;
- la conferenza internazionale Q2B organizzata da QC-Ware[63] che rappresenta una buona opportunità per entrare a contatto sia con i progressi scientifici sia con i maggiori player commerciali.

4.2 Gli standard

Lo sviluppo di standard industriali è di fondamentale importanza per il diffondersi delle tecnologie e per accelerare il mercato in quanto essi favoriscono l’interoperabilità tra apparati di diversi *vendor* grazie alla definizione di interfacce e specifiche per le differenti componenti. Anche per le tecnologie quantistiche ci sono differenti iniziative volte a favorire la standardizzazione a livello internazionale o locale, con contributi di organismi statali o commerciali.

Le aree di standardizzazione sono molteplici e vanno da aspetti come le tecnologie abilitanti fino alle componenti applicative.

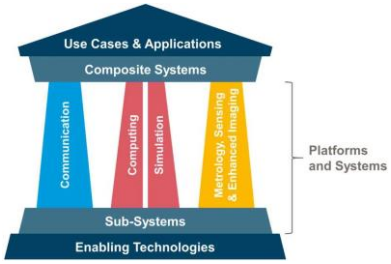


Figura 12 - CEN/CENELEC Standardization Roadmap on QT: 2023-03

L’Unione europea è caratterizzata dalla presenza di enti come ETSI[64] o CEN/CENELEC[65] (un *focus group* sulle tecnologie quantistiche è stato istituito nel 2020) che cooperano con altre organizzazioni internazionali per la creazione di standard globali. ISO[66] ha un gruppo di lavoro dedicato (ISO/IEC JTC 1/WG 14) mentre IEEE[67] ha lanciato diverse iniziative per il benchmarking.

61 https://www.osservatori.net/it/ricerche/osservatori-attivi/quantum-computing-communication
62 https://www.insidequantumtechnology.com/
63 https://www.qcware.com/
64 https://www.etsi.org/about
65 https://www.cencenelec.eu/about-cenelec
66 https://www.iso.org/about-us.html
67 https://www.ieee.org/about/index.html

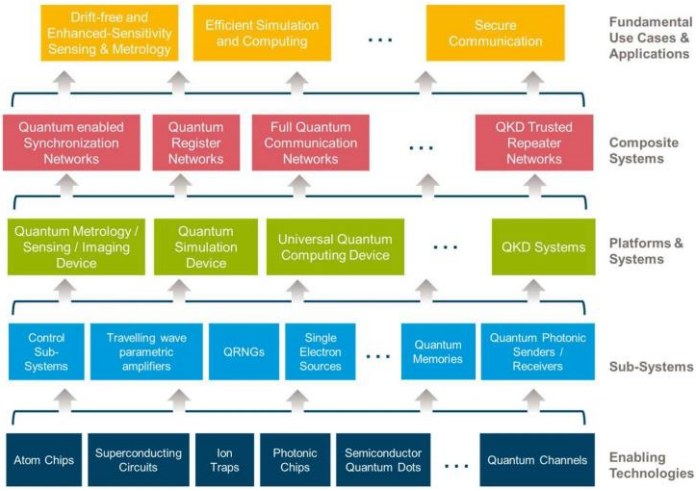


Figura 13: Ambito di definizioni di standard per le tecnologie quantistiche[68]

4.2.1 Standard per il quantum *computing*

L’assenza di standard di specifiche tecnologiche in questo ambito è conseguenza del loro scarso livello di maturità e può scoraggiare chi valuti di investire nell’adozione di progetti che coinvolgano la sperimentazione di elaborazione quantistica. Allo scopo di ridurre la confusione generata dall’uso di concetti con differenti significati e facilitare la comunicazione, è in via di definizione uno standard (ISO/IEC DIS4879, *Information technology – Quantum computing – Terminology and vocabulary*) che descrive i concetti di base (hardware, software e applicazioni) presenti nel quantum *computing*.

Anche i seguenti standard sono in corso di definizione: ISO/IEC TR 18157 (*Information technology – Introduction to quantum computing*) che fornisce una introduzione al quantum *computing* e relative tecnologie, ISO/IEC PWI 18670 (*Information technology — Reference framework for quantum computing service platforms)*, ISO/IEC PWI 18660 (*Information technology — Quantum machine learning datasets*) che fornisce un benchmark standard per gli algoritmi di apprendimento automatico e ISO/IEC PWI 20153 (*Quantum Simulation — Taxonomy of quantum simulator architectures and quantum simulation programming*).

4.2.2 Standard per QKD

A livello globale si osserva una intensa attività volta alla creazione di standard in ambito QKD, nonostante si tratti di una tecnologia relativamente nuova. In particolare, l’interesse si è focalizzato nella definizione di *use case*, specifiche di sicurezza e interoperabilità.

L’Unione europea è presente nei lavori di standardizzazione di ISO, IEEE, ETSI e CEN-CENELEC[69]. In particolare:

- *ISO/IEC 23837: Security requirements, test and evaluation methods for quantum Key Distribution (2023)* - gli standard vengono divisi in due parti principali. Nella prima parte

[68] “Towards European Standards for Quantum Technologies” https://arxiv.org/ftp/arxiv/papers/2203/2203.01622.pdf

[69] https://www.iso.org/committee/10138914.html, https://quantum.ieee.org/, https://www.etsi.org/technologies/quantum-safe-cryptography, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

vengono specificati i requisiti funzionali base e l’insieme dei test e dei metodi di valutazione condivisi per la QKD. In particolare, vengono esplicitati quali siano le componenti network e di quantum optics standard e le tecniche di implementazione di un protocollo di QKD. All’interno della seconda parte vengono specificati i test e i metodi di valutazione dei requisiti di sicurezza e delle implementazioni sopra menzionate;

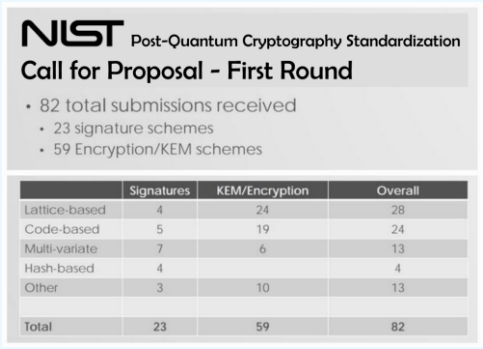
- *ETSI GS QKD 014: Protocol and data format of REST-based key delivery API* – specifiche per la comunicazione tra client e i moduli QKD per l’utilizzo delle chiavi generate tramite protocollo di distribuzione quantistica.

4.2.3 La standardizzazione degli algoritmi post-quantum

Nel dicembre del 2016, il NIST ha avviato un processo di standardizzazione[70] di algoritmi crittografici capaci di resistere ad attacchi basati su computer quantistici, lanciando una competizione internazionale aperta a candidati provenienti da aziende ed enti di ricerca di tutto il mondo.

NIST Post-Quantum Cryptography Standardization

Il termine per la presentazione delle candidature, 82 in questa prima fase (Tabella 4), è stato inizialmente fissato al 30 novembre 2017. Le analisi sulle candidature sono state discusse pubblicamente e approfondite attraverso il PQC forum che vanta 1300 membri da ogni parte del mondo. Dopo solo tre settimane la community ha compromesso 12 schemi mentre un tredicesimo è stato scartato per carenze nei requisiti di ammissione. Nel dicembre 2017, i 69 candidati rimasti sono stati ufficialmente ammessi a partecipare alla competizione.



	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	23	59	82

Tabella 4 - Le proposte pervenute al NIST classificate per tipologia

Dall’11 al 13 aprile 2018 si è tenuto a Fort Lauderdale il primo “NIST Workshop on PQC Standardization”, dove i 69 candidati sono stati presentati e discussi pubblicamente. I candidati ammessi alla competizione vedevano coinvolti 263 ricercatori provenienti da 24 Paesi diversi, tra cui anche l’Italia. La valutazione di tutti i candidati è iniziata subito dopo l’annuncio della loro ammissione e si è protratta per oltre un anno. Essa è stata condotta dal NIST, ma col contributo fondamentale della comunità internazionale, che ha analizzato indipendentemente tutti i candidati e condiviso i risultati delle analisi tramite una mailing list pubblica messa a disposizione dal NIST.

A oltre un anno di distanza, il 30 gennaio 2019 il NIST ha annunciato 26 candidati ammessi al secondo turno della competizione. Tra di essi, otto vedono il coinvolgimento di ricercatori italiani, ovvero: BIKE, Classic

[70] https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms

McEliece, CRYSTALS-KYBER, HQC, LEDAcrypt, NewHope e SIKE per la cifratura e lo scambio di chiavi, oltre a Picnic per la firma digitale. LEDAcrypt è l’unico interamente sviluppato da ricercatori italiani.

Nell’agosto del 2019 si è tenuto un secondo workshop dove sono stati ripresentati e rianalizzati i candidati rimasti. Con l’avvio del secondo turno di valutazione, il NIST ha chiesto nuovamente alla comunità internazionale di focalizzare l’attenzione su questo gruppo ristretto di 26 proposte, che sono state sottoposte a ulteriore analisi per circa un anno, allo scopo di verificarne ulteriormente la sicurezza e, al tempo stesso, studiarne le prestazioni su sistemi reali.

Il secondo round si è concluso nel luglio 2020. Gli algoritmi scelti come finalisti del terzo turno sono stati Classic McEliece, CRYSTALS-KYBER, NTRU e SABER per la cifratura e CRYSTALS-DILITHIUM, FALCON e Rainbow per la firma digitale. Inoltre, otto algoritmi candidati alternativi accedono anch’essi al terzo turno: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic e SPHINCS+.

Il terzo e ultimo round si è chiuso nel luglio 2022. Il processo di selezione ha identificato gli algoritmi ufficiali per la standardizzazione (CRYSTALS-Kyber per la cifratura e CRYSTALS-DILITHIUM, FALCON e SPHINCS+ per la firma digitale), nonché un set di algoritmi alternativi che continueranno a essere valutati in un quarto turno di analisi.

Inoltre, quattro degli algoritmi alternativi candidati per la creazione di chiavi sono passati a una quarta fase di valutazione: BIKE, Classic McEliece, HQC e SIKE. Questi algoritmi sono ancora in fase di valutazione per una futura standardizzazione, anche se alcuni - come il SIKE - sono già stati ritenuti non sicuri.

Molti di questi algoritmi di crittografia post-quantistica richiedono chiavi di dimensioni maggiori rispetto agli algoritmi classici comunemente utilizzati e richiedono di considerare anche l'efficienza computazionale, la dimensione della firma e altri parametri[71].

Gli algoritmi sono in corso di standardizzazione sono CRYSTALS-KYBER per la cifratura e CRYSTALS-Dilithium, FALCON e SPHINCS+ per la firma digitale. Di quest’ultimi, il NIST raccomanda l’uso di CRYSTALS-Dilithium come algoritmo principale e FALCON per applicazioni che richiedono firme più piccole. SPHINCS+ risulta meno effciente degli altri due ma è stato incluso perché basato su problemi matematici differenti dagli altri tre.

In futuro, il NIST pubblicherà un nuovo invito a presentare proposte per algoritmi di firma digitale a chiave pubblica per aumentare e diversificare il suo portafoglio di firme.

[71] I sistemi crittografici proposti per la selezione del NIST sono basati sulla matematica dei reticoli (lattices), codici a correzione d’errore, polinomi multivariati, funzioni hash e isogenie con vantaggi e svantaggi. Ad esempio, le famiglie di algoritmi crittografici basati su codici godono di una lunga storia di verifica “pubblica”, mentre la crittografia basata su reticoli (lattices) offre algoritmi estremamente veloci ma la maggiore dimensione dei dati in gioco potrebbe rivelarsi problematica. Il NIST, quindi, si è orientato a standardizzare differenti algoritmi per rendere flessibile il loro utilizzo a seconda del contesto.

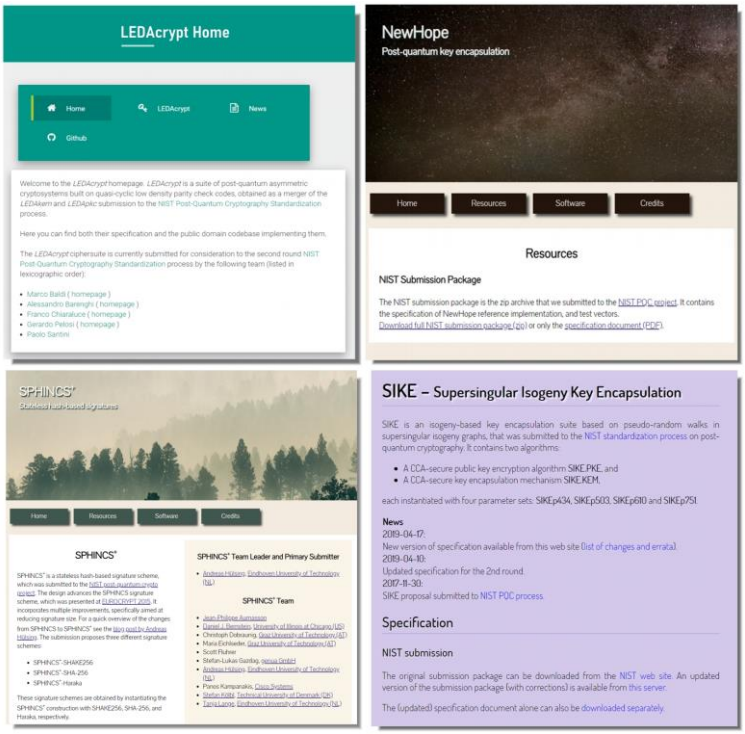


Figura 14: Le homepage di alcuni degli schemi di cifratura tuttora in competizione

4.3 Le istituzioni

4.3.1 Il contesto internazionale

Molti degli investimenti, a livello globale, sulla ricerca e sulla diffusione delle tecnologie quantistiche sono effettuati dal settore pubblico e sono in costante aumento: oltre 30 nazioni sono coinvolte attivamente nelle tecnologie quantistiche e i due terzi di queste nazioni hanno formulato una politica ufficiale sul quantum. L’interesse del settore pubblico è dovuto alla consapevolezza della necessità di mettere in sicurezza le infrastrutture nazionali critiche dai possibili attacchi cyber, sempre più fondati su tecnologie innovative.

Dalle stime di QURECA[72] riportate anche dal World Economic Forum[73], l’investimento in ricerca e sviluppo di tecnologie quantistiche finanziato dal settore pubblico ammonta complessivamente a 40 miliardi di euro distribuiti su differenti orizzonti temporali.

[72] https://www.qureca.com/quantum-initiatives-worldwide-2024/

[73] https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

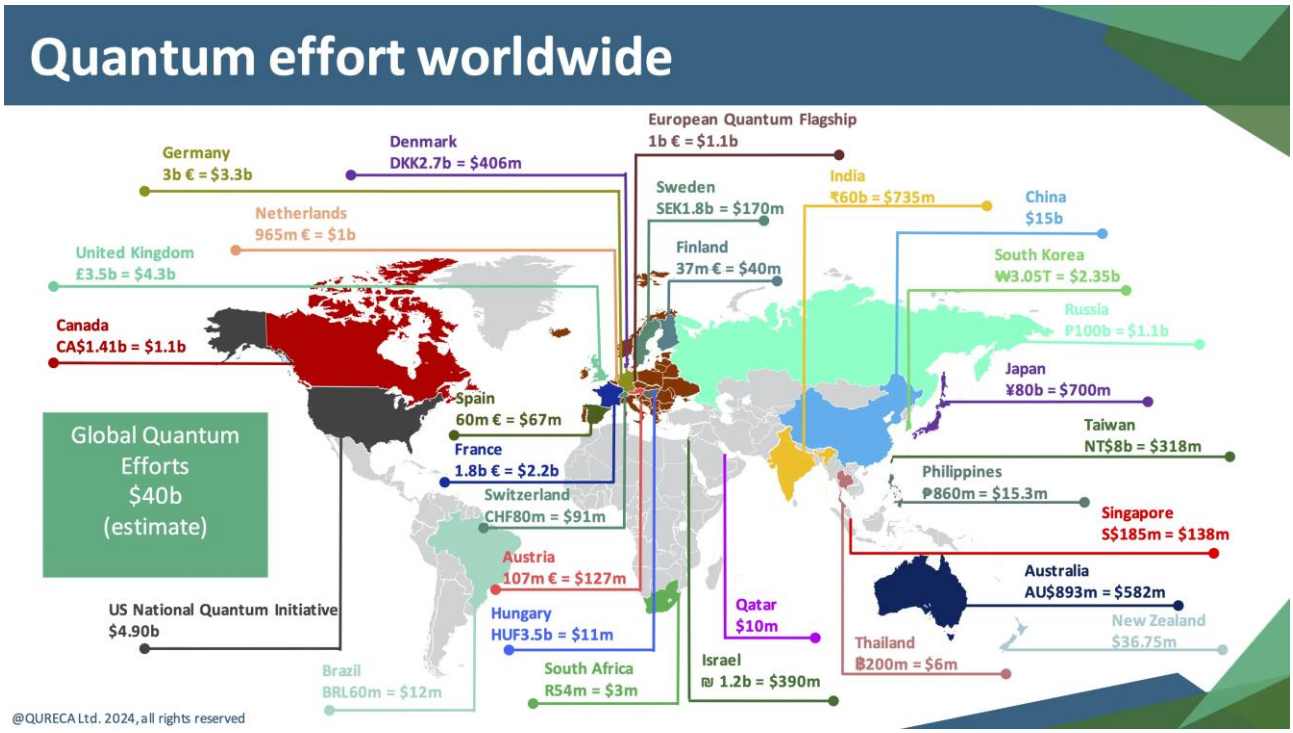


Figura 15: investimenti pubblici in tecnologie quantistiche[74]

Diversi paesi hanno definito una strategia nazionale per le tecnologie quantistiche, con lo stanziamento di fondi specifici. Una breve sintesi di alcune di esse è riportata al paragrafo 8.1.
Tutte queste iniziative hanno in comune il finanziamento di attività di ricerca e sviluppo, la collaborazione con l’industria, i fornitori di tecnologia e infrastrutture, la collaborazione internazionale con l’istituzione di partnership bilaterali o multilaterali e la formazione accademica per alimentare risorse umane preparate nei prossimi decenni ad affrontare le sfide del mondo quantistico.

4.3.1.1 La strategia USA

Tra le iniziative più rilevanti, va segnalata quella in capo all’amministrazione Biden che invita a predisporre l’adozione degli algoritmi PQC annunciati dal NIST nel luglio 2022. Nel dicembre 2022, il presidente degli Stati Uniti ha firmato il *Quantum Computing Security Preparations Act*, che stabilisce una serie di obblighi per le agenzie federali per preparare la loro transizione alla crittografia post-quantistica con una *roadmap* stringente[75].

US National Quantum Initiative
L’America ha lanciato nel 2018 la propria strategia per le tecnologie quantistiche con il National Quantum Initiative Act – NQIA che prevede uno stanziamento di oltre 1,2 miliardi di dollari per un primo periodo di cinque anni, al quale si sono aggiunti gli stanziamenti stabiliti dai diversi piani di investimento definiti nelle altre iniziative di spesa. Successivamente il NQIA è stato integrato o emendato da altri atti legislativi in

[74] “Overview of Quantum Initiatives Worldwide 2024”, QURECA 1 Aprile 2024, https://www.qureca.com/quantum-initiatives-worldwide-2024/

[75] Memo-on-Migrating-to-Post-Quantum-Cryptography, Executive Office of the President, november 2022

considerazione delle implicazioni delle tecnologie quantistiche in campo commerciale e della difesa. L’obiettivo della National Quantum Initiative è quello di accelerare la ricerca e lo sviluppo nelle tecnologie quantistiche per la sicurezza economica e nazionale degli Stati Uniti, con il coinvolgimento anche del settore civile, della difesa e dell’intelligence.

Come anche ribadito nell’Executive Order 14073 firmato dal presidente Biden nel maggio 2022, l’iniziativa prevede nel complesso un coinvolgimento di tutti i Governi Federali e fornisce un *framework* per rafforzare e coordinare tali attività tra gli US Departments e le agenzie, il settore industriale privato e la comunità accademica.

Le attività di ricerca sono portate avanti dalle agenzie menzionate negli atti legislativi sopra indicati, quali, ad esempio, il National Institute of Standards and Technology (NIST), il National Science Foundation (NSF), il Department of Energy (DOE), la National Aeronautics and Space Administration (NASA), il Department of Defense (DOD).

Oltre all’Executive Order già menzionato, nel maggio 2022 il presidente Biden ha anche firmato un National Security Memorandum con la descrizione delle azioni da intraprendere da parte del governo federale per l’adozione di una PQC cyber security per difendersi dalle minacce della crittografia quantum, in linea con i quattro standard approvati dal NIST nel luglio 2022. In tale contesto il NIST ha avuto anche il compito di implementare un progetto di migrazione PQC per il governo federale e per le industrie.

Nell’ambito delle direttive degli Stati Uniti è necessario anche citare l’Executive Order del 2023 con il quale l’amministrazione Biden ha proibito gli investimenti americani in settori cinesi sensibili, tra cui quello delle tecnologie quantistiche.

4.3.2 Il contesto europeo

In Europa Paesi Bassi, Germania, Francia, Danimarca e Irlanda hanno definito una strategia nazionale, Spagna e Svezia stanno lanciando le loro, mentre altri paesi hanno programmi di investimenti dedicati alle tecnologie quantistiche (ad esempio l’Austria). Dall’ultimo rapporto McKinsey[76] sugli investimenti pubblici in tecnologie quantistiche, nel 2022 la Germania ha stanziato più fondi, seguita dalla Francia, dall’Unione europea e dai Paesi Bassi.

La Commissione europea[77] ha promosso investimenti per lanciare diverse iniziative a lunga durata, (tra le principali “Quantum Flagship”[78], EuroHPC, EuroQCI) e uno specifico centro di competenza (ECCC) al fine di coordinare le differenti iniziative tra istituti di ricerca, industria ed enti pubblici.

Nel febbraio 2023 è stato pubblicato un documento strategico[79] legato allo sviluppo delle tecnologie quantistiche in ambito europeo con l’obiettivo di armonizzare *roadmap* e obiettivi per il mondo della scienza e dell’industria. Il documento prevede alcuni obiettivi a medio e lungo termine per garantire soluzioni affidabili e disponibili all’intero sistema.

[76] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf

[77] https://digital-strategy.ec.europa.eu/en/policies/quantum

[78] https://qt.eu/about-quantum-flagship/

[79] https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf?m=1707900786&

4.3.2.1 Quantum Flagship

European Quantum Flagship è un’iniziativa dell’Unione europea volta a promuovere la ricerca e lo sviluppo nel campo delle tecnologie quantistiche. Lanciata a ottobre 2018, mira a consolidare e coordinare gli sforzi di ricerca in tutta Europa per accelerare i progressi nelle tecnologie quantistiche e favorire la leadership europea in questo settore emergente e strategico.

Con un budget di 1 miliardo di Euro e un orizzonte temporale di 10 anni, viene finanziata la ricerca su diversi aspetti dell’ambito quantistico: *sensing*, comunicazioni, calcolo e simulazione. È prevista, tramite l’introduzione di programmi di lavoro, la collaborazione tra enti di ricerca, università, aziende e istituzioni governative di vari paesi europei, per sfruttare al massimo le competenze e le risorse disponibili in Europa e promuovere l'innovazione nelle tecnologie quantistiche.

4.3.2.2 ECCC

L’European Cybersecurity Competence Centre (ECCC) mira ad aumentare le capacità e la competitività dell'Europa in materia di cyber sicurezza, collaborando con una rete di centri nazionali di coordinamento (NCC) per costruire una forte comunità di cyber sicurezza. Con sede a Bucarest, svilupperà e attuerà, insieme agli Stati membri, all'industria e alla comunità tecnologica della cyber sicurezza, un'agenda comune per lo sviluppo della tecnologia e per la sua ampia diffusione in settori di interesse pubblico e nelle imprese, in particolare nelle PMI.

ECCC avrà anche il compito di indirizzare investimenti strategici mettendo a disposizione degli Stati membri le risorse dell'UE e indirettamente dell'industria, per migliorare e rafforzare le capacità in ambito cyber sicurezza. Il Centro svolgerà un ruolo fondamentale nella realizzazione degli obiettivi di cyber sicurezza del *Digital Europe Programme*[80] e dell’*Horizon Europe programme*[81].

4.3.2.3 EuroQCI

La Commissione europea collabora con i 27 Stati membri dell’Unione europea e con l’Agenzia Spaziale Europea (ESA) per progettare, sviluppare e distribuire un’infrastruttura di comunicazione quantistica sicura ed efficiente in tutta l’Unione, l’EuroQCI (*European Quantum Communication Infrastructure*). L’obiettivo è proteggere i dati sensibili e le infrastrutture critiche integrando i sistemi quantistici nelle infrastrutture di comunicazione esistenti e fornire un ulteriore livello di sicurezza basato sulla fisica quantistica.

L’EuroQCI sarà composto da un segmento terrestre, basato su reti di comunicazione in fibra ottica, che collegano siti strategici a livello nazionale e transfrontaliero, e da un segmento spaziale basato sui satelliti. Sarà parte integrante dell'IRIS2, il nuovo sistema di comunicazione spaziale sicuro dell'UE.

Il progetto è stato avviato nel 2019 ed è finanziato con 1 miliardo di euro su un orizzonte temporale di 10 anni.

[80] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[81] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

4.3.2.4 EuroHPC

Il progetto EuroHPC (*European High Performance Computing*) rappresenta il pilastro portante della strategia industriale dell’Unione europea nel campo del supercalcolo e dell’elaborazione dei dati. EuroHPC prevede il finanziamento di progetti innovativi, con il duplice obiettivo di sviluppare un’infrastruttura di supercalcolo paneuropea e di sostenere la cooperazione nella ricerca scientifica avanzata al fine di aumentare la competitività industriale e di garantire, al contempo, l’autonomia tecnologica e digitale europea.

La componente quantum del progetto sarà finanziata con 1,5 miliardi di euro fino al 2027, su un totale di 5 miliardi di euro.

Nell’ottobre 2022 sono stati individuati sei siti europei (tra cui il CINECA, in Italia) che ospiteranno quantum computer realizzati con differenti tecnologie. Questo rappresenta il primo passo verso la costruzione di una infrastruttura di calcolo quantistico europeo che ha lo scopo di essere accessibile al mondo accademico e industriale per la crescita collettiva dell’unione.

4.3.2.5 OpenQKD

OpenQKD (Open Quantum *Key Distribution*) è un’iniziativa europea che mira a sviluppare e implementare tecnologie di distribuzione di chiavi quantistiche (QKD) in modo aperto e interoperabile. Il team è multidisciplinare, vi fanno parte i principali produttori europei di apparecchiature di telecomunicazione, utenti finali, fornitori di infrastrutture critiche, operatori di rete, fornitori di apparecchiature QKD, professionisti della sicurezza digitale e scienziati provenienti da 13 paesi dell’Unione europea.

4.3.2.6 Post quantum cryptography in Europa

La Commissione europea si è espressa solo molto recentemente[82] sull’utilizzo degli algoritmi post-quantum. In particolare, attraverso una raccomandazione specifica:

- invita gli Stati membri a procedere quanto prima alla migrazione delle loro infrastrutture e dei loro servizi digitali attuali per le pubbliche amministrazioni, nonché di altre infrastrutture critiche, verso la crittografia post-quantistica;
- incoraggia gli Stati membri a elaborare una strategia globale per l'adozione della crittografia post-quantistica al fine di garantire una transizione coordinata e sincronizzata tra i diversi Stati membri e i rispettivi settori pubblici;
- indica la necessità di seguire una *roadmap* che contenga l'elenco delle azioni che gli Stati membri devono intraprendere con un calendario chiaro per le diverse fasi e i diversi traguardi da raggiungere;
- incoraggia gli Stati membri a collaborare a livello di UE a stretto contatto con gli esperti dell'Unione in materia di cibersicurezza, con il gruppo di cooperazione NIS e con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sulla valutazione e sulla selezione degli

[82] https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography

algoritmi di crittografia post-quantistica adeguati e sulla loro adozione come norme dell'UE ai fini di un'attuazione armonizzata in tutta l'Unione;

- subito dopo la pubblicazione della presente raccomandazione gli Stati membri sono invitati a istituire un sottogruppo sulla crittografia post-quantistica a norma della decisione di esecuzione (UE) 2017/179 della Commissione e a nominare rappresentanti esperti che dovrebbero lavorare in stretta collaborazione con la Commissione ed essere incaricati di definire ed elaborare la tabella di marcia per l'attuazione coordinata della crittografia post-quantistica stabilendo il limite temporale di due anni dalla pubblicazione della raccomandazione.

Tra i paesi del vecchio continente non ci sono iniziative pubbliche di rilevo, altre istituzioni europee avevano pubblicato specifiche raccomandazioni come il *German Federal Office for Information Security* che nel 2021 ha diffuso un documento di raccomandazioni[83] indirizzato ad aziende pubbliche e private, tra l’altro, referenziato dalla stessa Commissione europea[84].

4.4 Il contesto nazionale

L’Italia può vantare diversi centri di ricerca attivi nel campo delle tecnologie quantistiche. Università ed enti di ricerca seguono ambiti di ricerca evoluti sia nel campo del calcolo quantistico che in quello della sicurezza. In particolare si segnalano: La Sapienza di Roma (*qubit* fotonici), l’Università di Padova (trapped ions), l’Università Federico II (*qubit* superconduttori) e il CINECA (sperimentazione dell’elaboratore Pasqal e soluzioni ibride per sfruttare la computazione quantistica come acceleratore di quella classica) e INRIM (creazione di una rete quantistica nazionale).

Il rapporto dell’Osservatorio del Politecnico di Milano sul 2023[85] riporta che i fondi stanziati nel nostro paese dal settore pubblico (140 milioni per il triennio 2023-2025) appaiono largamente insufficienti non solo rispetto agli stanziamenti dei paesi del Nord America e della Cina ma anche rispetto a quelli degli altri paesi europei (si parla di miliardi in orizzonti temporali decennali, cfr. Figura 15).

In Italia si assiste, inoltre, sempre secondo le stime dell’Osservatorio, a una limitazione di investimento (circa 6 milioni di euro) nel settore privato dove ci si confronta, con maggior rilievo nell’ultimo anno, con l’assegnazione di risorse umane e budget limitati senza una strategia di medio-lungo termine.

[83] https://www.bsi.bund.de/EN/Topics/Crypto/Cryptography/PostQuantumCryptography/post_quantum_cryptography_node.html

[84] ENISA, Post Quantum Cryptography Study, october 2022

[85] L’Osservatorio “Quantum Computing & Communication” del Politecnico di Milano si qualifica come “un punto di riferimento precompetitivo sul tema a livello italiano, coinvolgendo una community di aziende interessate, lato domanda e offerta di tecnologia, e di esperti a livello italiano e internazionale”.

4.4.1 Le iniziative del settore pubblico

Il Piano Nazionale di Ripresa e Resilienza (PNRR) è articolato in sette missioni[86]. Nell’ambito della componente “Dalla ricerca al business” della missione 4 “Istruzione e Ricerca” il PNRR stanzia 1,6 miliardi di euro per creare centri nazionali di ricerca su temi di importanza strategica, tra cui simulazioni, calcolo e analisi dei dati ad alte prestazioni, agritech, sviluppo di terapia genica e farmaci con tecnologia a RNA, mobilità sostenibile e biodiversità[87]. I centri nazionali sono aggregazioni di università, enti di ricerca e imprese, organizzati con una struttura di tipo “*hub and spoke*”, con l’*hub* che si occupa di attività di gestione e coordinamento e gli *spoke* di ricerca.

Nome Centro Nazionale	Proponente	Sede Hub	Numero Soggetti Partecipanti Totali	Numero Università-enti pubblici di ricerca-organismi di ricerca	Numero Imprese	Finanziamento concesso (in euro)
National Centre for HPC, Big Data and Quantum Computing	Istituto Nazionale di Fisica Nucleare (INFN)	Casalecchio di Reno (BO)	49	34	15	319.938.979,26
National Research Centre for Agricultural Technologies (Agritech)	Università degli Studi di Napoli Federico II	Napoli	46	32	14	320.070.095,50
Sustainable Mobility Center (Centro Nazionale per la Mobilità Sostenibile – CNMS)	Politecnico di Milano	Milano	49	25	24	319.922.088,03
National Biodiversity Future Center - NBFC	Consiglio Nazionale delle Ricerche (CNR)	Palermo	48	41	7	320.026.665,79
National Center for Gene Therapy and Drugs based on RNA Technology	Università degli Studi di Padova	Padova	49	32	17	320.036.606,03

Figura 16: tratto dal comunicato del MUR[88]

In particolare, il PNRR prevede un investimento di 320 milioni di euro in tre anni per la creazione di un Centro Nazionale per HPC, Big Data e Quantum Computing; il progetto vede la partecipazione di 34 tra università ed enti pubblici di ricerca e 15 imprese. Lo spoke 10[89], dedicato al quantum computing, prevede un investimento di 30 milioni di euro.

Si segnalano nel seguito alcune iniziative degne di interesse.

86 "Digitalizzazione, Innovazione, Competitività, Cultura", "Rivoluzione Verde e Transizione Ecologica", "Infrastrutture per una Mobilità Sostenibile", "Istruzione e Ricerca", "Inclusione e Coesione", "Salute", "RePowerEU".

87 “PNRR e quantum computing: 320 milioni di euro per il centro nazionale sul supercalcolo” (osservatori.net)

88 https://www.mur.gov.it/it/news/mercoledi-15062022/pnrr-nascono-i-5-centri-nazionali-la-ricerca

89 https://www.supercomputing-icsc.it/spoke-10-quantum-computing/

Il National Quantum Science and Technology Institute[90] (NQSTI) è un consorzio formato da 20 tra centri di ricerca, università e industrie high-tech italiane che favorisce la collaborazione fra enti che svolgono ricerca nel campo della scienza e della tecnologia quantistica in Italia. Il NQSTI coordina i fondi pari a 116 milioni di euro di uno degli investimenti della missione 4 “Istruzione e ricerca” – Componente 2 “Dalla ricerca all’impresa” dedicato ai “Partenariati allargati a Università, centri di ricerca, imprese e finanziamento” nell’ambito delle scienze e tecnologie quantistiche.

Il Quantum Computing Lab del CINECA è una iniziativa volta a sviluppare strumenti di calcolo quantistico per l'elaborazione e il calcolo delle informazioni[91]. Attualmente, il CINECA non dispone di un computer quantistico, ma ha deciso di integrare la sua offerta di calcolo ad alte prestazioni con risorse di calcolo quantistico, sia attraverso ore di calcolo su macchine quantistiche in cloud, sia attraverso risorse HPC classiche in grado di emulare il calcolo quantistico.

Il progetto QUID (Quantum Italy Deployment) è la realizzazione italiana della European Quantum Communication Infrastructure (EuroQCI), promossa dalla Commissione europea con l'obiettivo di creare un'infrastruttura europea per la comunicazione quantistica. Il progetto mira a sviluppare nodi in reti di comunicazione quantistica metropolitane (QMAN), interconnessi attraverso l'Italian Quantum Backbone, un'infrastruttura che copre il territorio italiano e distribuisce segnali standard di tempo e frequenza utilizzando fibre ottiche commerciali[92].

4.4.2 Le iniziative del settore privato

In Italia, il settore delle tecnologie quantistiche è ancora limitato a poche realtà, nonostante alcune di esse abbiano ricevuto riconoscimenti di livello internazionale di cui si citano alcuni esempi:

- Telsy è il centro di competenza di Cybersecurity e Crittografia di TIM Enterprise che, insieme con la partecipata QTI Quantum Telecommunications Italy, fornisce sistemi di crittografia end-to-end compatibili con le attuali infrastrutture di telecomunicazione per applicazioni private, governative e militari;
- LevelQuantum è una start up che sfrutta la tecnologia quantistica nel campo della sicurezza informatica. La start up è stata recentemente selezionata dalla NATO nel suo programma di accelerazione DIANA (Defence Innovation Accelerator for the North Atlantic) che ha l’obiettivo di promuovere diverse tecnologie innovative;
- QBrain è una start up che sviluppa e fornisce soluzioni software quantistiche per le aziende, facendo uso di un motore di Intelligenza Artificiale progettato per ottimizzare sia gli algoritmi quantistici sia l’hardware;
- G2Q Computing è una start up specializzata nel calcolo scientifico, che sviluppa applicazioni ibride (quantistiche/classiche) avanzate per risolvere problemi complessi e migliorare le performance.

Da sottolineare in tale ambito tutte le iniziative di finanziamento pubblico e privato rese accessibili dagli incubatori di innovazione, come quello del Politecnico di Torino I3P, del Politecnico di Milano

[90] https://nqsti.it/
[91] https://www.quantumcomputinglab.cineca.it/
[92] https://www.quantumlab.it/avvio-progetto-quid-quantum-italy-deployment/

PoliHub e la rete italiana dei Business Incubation Center dell’Agenzia spaziale europea. Gli incubatori forniscono servizi di consulenza strategica, coaching, mentoring e supporto al fundraising.

4.4.3 L’offerta accademica

Diverse università italiane hanno attivato corsi di laurea magistrale, master o dottorati di ricerca in tecnologie quantistiche, in collaborazione anche con enti di ricerca e fondazioni. In particolare:

- l’Università Federico II di Napoli ha attivato il corso di laurea magistrale in *Quantum Science and Engineering* (durata due anni) con l’obiettivo di formare esperti di tecnologie quantistiche con competenze multidisciplinari (dalla fisica all'informatica, dall'ingegneria elettronica a quella dell'informazione e delle comunicazioni). Gli studi possono poi continuare con il *PhD Quantum Technologies* della durata di tre anni attivato presso l'Università in consorzio con il CNR di Firenze e l’Università di Camerino;
- il Politecnico di Torino offre un corso di laurea magistrale in *Quantum Engineering* con l’obiettivo di fornire una preparazione multidisciplinare, con particolare riferimento a tre ambiti applicativi: computazione, comunicazione e sensoristica quantistica. Il Politecnico ha inoltre avviato nel 2022 un Master di II livello in *Quantum Communication and Computing* in collaborazione con l’Istituto Nazionale di Ricerca Metrologica e Fondazione LINKS[93];
- il Politecnico di Milano ha avviato nell’autunno del 2022 il corso di laurea magistrale in *High Performance Computing Engineering* della durata di due anni, con l’obiettivo di fornire una solida preparazione nelle principali tecnologie e architetture informatiche per il supercalcolo, nel quantum *computing* e nella modellazione matematico-statistica di problemi complessi;
- presso l’Università la Sapienza di Roma è attivo il *Master di Optics and Quantum Information*, giunto alla sua ottava edizione, primo nato in Italia e uno dei primi in Europa. Presso l’Università è presente il *Quantum Computing Lab* dedicato allo studio e alla realizzazione sperimentale di protocolli di computazione con sistemi fotonici. L’università è a capo anche di EPIQUE, progetto di ricerca finanziato con 10 milioni di euro dalla Commissione europea realizzato da 18 partner di 12 paesi (tra cui il Consiglio nazionale delle ricerche e l’Università degli Studi di Firenze) che ha come obiettivo quello di studiare in modo approfondito il potenziale offerto dallo sviluppo di piattaforme di calcolo quantistico fotonico e di realizzare un computer quantistico europeo basato sui fotoni;
- l’Università Ca’ Foscari Venezia offre un corso di laurea magistrale in *Engineering Physics* con un indirizzo di studio su *Quantum Science and Technology* e ha attivato un master di primo livello in Quantum *Machine Learning* con l’obiettivo di approfondire i temi del quantum *computing*, con un’impostazione multidisciplinare che prevede competenze di quantum *computing*, *machine learning*, matematica statistica, fisica, informatica, economia e finanza;

[93] LINKS è una Fondazione nata da un accordo tra Compagnia di San Paolo e Politecnico di Torino che opera da più di 20 anni a livello nazionale e internazionale nell’ambito della trasformazione digitale con attività di ricerca applicata, innovazione e trasferimento tecnologico. https://linksfoundation.com/

- l’Università di Trieste in collaborazione con il Centro internazionale di Fisica Teorica (ICTP) ha attivato il Master *Scientific and Data-Intensive Computing* con focus su *high performance computing*, *scientific computing* e quantum *computing,* della durata di due anni;
- l’Università di Trento nell’ambito del consorzio Q@TN ha lanciato un PhD in *Quantum Science and Technologies* della durata di tre anni con forti aspetti di interdisciplinarietà (fisica, matematica, informatica, ingegneria). Al consorzio Q@TN partecipano l’Università di Trento, la Fondazione Bruno Kessler, l’Istituto Nazionale di Fisica Nucleare e il CNR;
- l’Università di Pavia ha attivato un indirizzo di studio di Fisica delle tecnologie quantistiche nell’ambito del Corso di Laurea Magistrale in Scienze Fisiche, caratterizzato da un alto livello di interdisciplinarità (matematica, scienza dell’informazione, bioinformatica, chimica, ingegneria elettronica e delle comunicazioni), unendo gli aspetti più sperimentali e tecnologici a quelli più teorici. Nell’indirizzo si definiscono due profili, uno più fondamentale/teorico e uno più vicino alle applicazioni.

4.5 Il mercato e l’offerta tecnologica

4.5.1 Diffusione, maturità e prospettive delle tecnologie quantistiche

La maturità delle tecnologie quantistiche è un tema che merita un approfondimento dedicato per fornire elementi di concretezza in uno scenario spesso confuso dalle differenti notizie e dichiarazioni (cfr. Figura 17).

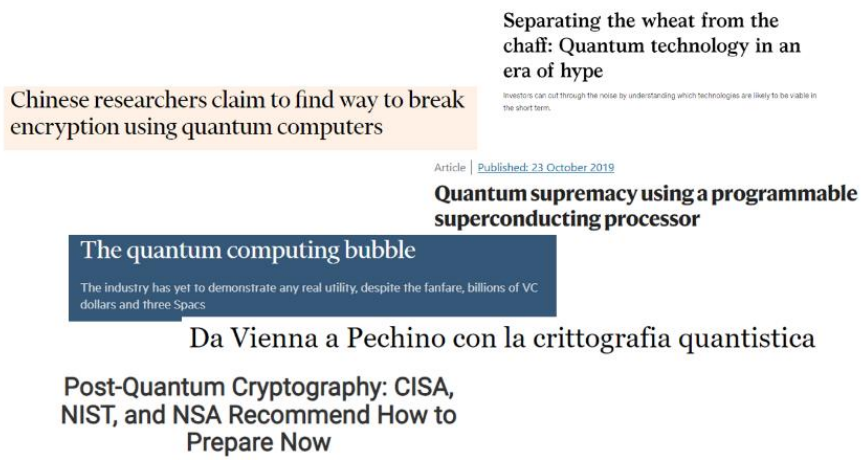


Figura 17 - Collage di alcuni titoli da testate di famosi giornali online

L’analisi nel tempo del numero di pubblicazioni scientifiche, brevetti, investimenti privati, start up evidenzia un andamento esponenziale nell’ultimo decennio e suggerisce opportunità di investimenti in tale ambito.

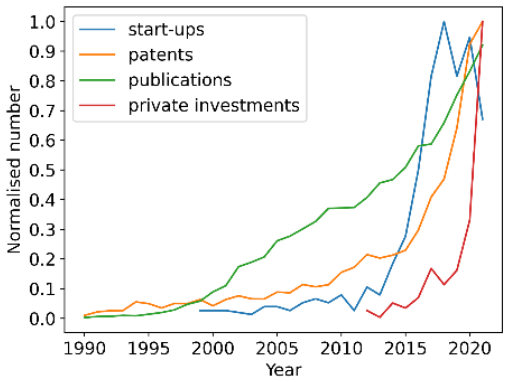


Figura 18 - Andamento di differenti indicatori di "quantum readiness"[94]

Elementi di maggior rilievo a favore dell’affermazione di queste tecnologie nel prossimo futuro possono essere così riassunti:

- le previsioni degli analisti che, seppure con forti scostamenti su alcune stime, indicano un progressivo aumento degli investimenti in questi settori; alcuni[76] stimano una crescita complessiva del mercato che porterebbe a raggiungere nel 2040 una quota di 106 miliardi di dollari, un terzo dei quali proveniente da investimenti pubblici;
- l’attenzione delle istituzioni in ambito internazionale con stanziamenti consistenti di fondi, progetti e pubblicazioni di strategie nazionali;
- le numerose iniziative di ricerca e sperimentazione in tutti gli ambiti descritti;
- l’emanazione di standard;
- la diffusione di modelli commerciali per la vendita di dispositivi e prodotti.

Per valutare la maturità tecnologica si fa comunemente riferimento alla scala TRL (Technology Readiness Level), nota dal mondo dell’aeronautica, e uniformemente diffusa[95].

Alcuni autori[94], sfruttando dati rivenienti da conferenze di settore, *assessment* e *roadmap* hanno realizzato un grafico (Figura 19) dello stato delle varie tecnologie e dell’orizzonte temporale richiesto per raggiungere il livello 9.

[94] Building a quantum-ready ecosystem, Abhishek Purohit, Maninder Kaur, https://arxiv.org/abs/2304.06843

[95] A. Olechowski, S. Eppinger, N. Joglekar, and K. Tomaschek, “Technology readiness levels: Shortcomings and improvement opportunities” Systems Engineering, vol. 23, 03 2020. I primi quattro livelli di questa scala (che va da 1 a 9) si riferiscono a fasi di ricerca ed esperimenti di laboratorio, il 5 e il 6 a presenza di prototipi mentre dal 7 al 9 si assiste a fasi di introduzione nel mercato con test e certificazioni a vari livelli.

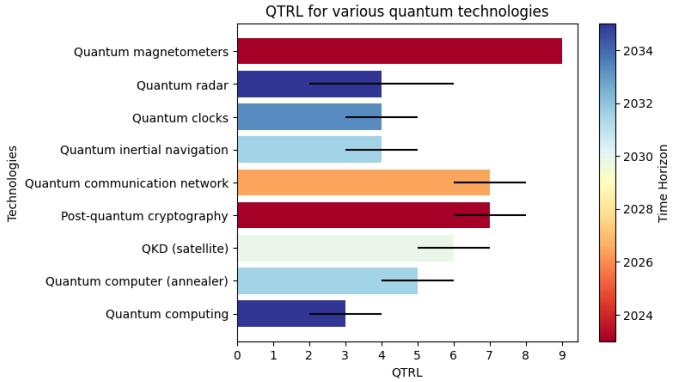


Figura 19 - Quantum TRL e aspettative temporali per differenti tecnologie quantistiche

Nonostante queste valutazioni presentino aspetti soggettivi, un dato generale è che si assiste a una offerta disomogenea dove alcune componenti (in particolare nel *sensing* e nel *communication*) rappresentano un livello di maturità più alto di altre. Per il quantum *computing*, come ripetutamente descritto, sono necessari ancora ingenti sforzi per superare le sfide poste dalla affidabilità, la capacità di correggere gli errori e la scalabilità. Per le componenti di quantum *key distribution,* quantum *random number generators* e quantum *sensing* invece, sono presenti svariati apparati sul mercato in grado di rispondere a differenti esigenze, grazie anche al ruolo di *system integrator* offerto da molti player soprattutto nell’ambito delle telecomunicazioni.

4.5.2 Quantum *Computing*

I dispositivi attualmente disponibili sono realizzati tramite un numero di *qubit* limitato, con poche interconnessioni e senza un meccanismo efficiente di correzione degli errori e, quindi, possono svolgere un numero limitato di operazioni.

Nelle figure seguenti sono rappresentati, suddivisi per differenti tecnologie, molti dei *vendor* e laboratori di ricerca che rientrano in questo ambito.

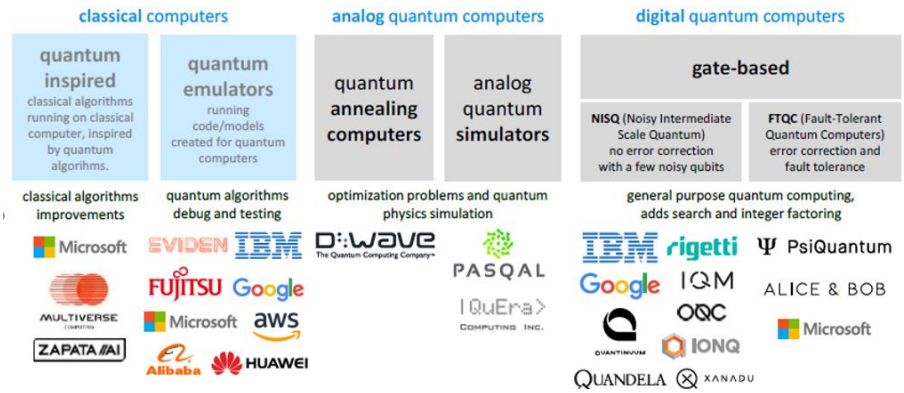


Figura 20 – Differenti *player* suddivisi per offerta tecnologica[96]

[96] Tratto da Olivier Ezratty “Understanding quantum Technologies – 2023” cc

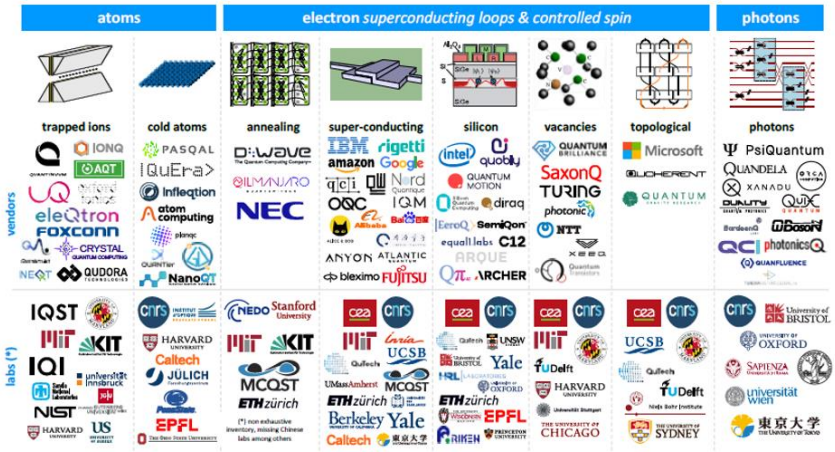


Figura 21 - Mappa di laboratori di ricerca e *vendor* commerciali suddivisi per tecnologia di *qubit* utilizzati[97]

In generale, il numero di *qubit* è utilizzato come unità di misura per rappresentare lo stato di avanzamento delle varie soluzioni ma il confronto è reso difficile dalla presenza di altre variabili (frequenza di errori, modalità di comunicazione tra *qubit*, ecc).

L’offerta di elaborazione quantistica è, principalmente, messa a disposizione in cloud dagli stessi produttori come IBM o D-Wave oppure offerta da service provider come Amazon o Google.

Di seguito, a titolo di esempio, alcune delle offerte disponibili allo stato della stesura del seguente resoconto:

TECNOLOGIA *QUBIT*	PROD	DISPONIBILITA’ WEB	SDK	NOTE
Superconduttori	IBM	https://docs.quantum.ibm.com/start/setup-channel#ibm-quantum-platform	QisKit	Disponibilità processore 16 *qubit* free / 100 *qubit* a pagamento
Superconduttori	Google	https://quantumai.google/cirq/	Cirq	Simulatore e interfaccia verso vari hardware
Ion trap	Alpine QT	https://www.aqt.eu/qc-systems/	AQT API	Simulatore gratuito, hardware a pagamento
Annealer	D-Wave	https://cloud.dwavesys.com/leap/signup/	Ocean	Cloud service for D-Wave
Diverse tecnologie	Azure	https://azure.microsoft.com/it-it/products/quantum	Q#	Interfaccia verso diversi produttori hardware
Diverse tecnologie	Amazon	https://aws.amazon.com/it/braket/	Amazon braket Python SDK	Interfaccia verso diversi produttori hardware – simulatori disponibili gratuitamente

[97] Tratto da Olivier Ezratty “Understanding Quantum Technologies” (a sua volta attualizzato da Gabriel Popkin in Science Mag, Dec. 2016)

4.5.3 Quantum *Programming*

I *framework* più importanti per il quantum *programming* sono di seguito brevemente descritti.

Qiskit [98]

Uno dei *framework* più popolari, sviluppato da IBM in Python. A oggi la community che supporta Qiskit si stima essere la più numerosa di tutti gli altri *framework* di quantum *programming*.

Esso offre la possibilità di:

- costruire circuiti anche sfruttando una vasta libreria di algoritmi quantistici per la risoluzione di una varietà di problemi, inclusi ottimizzazione, apprendimento automatico e crittografia;
- simulare circuiti quantistici su computer classici per testare i propri circuiti prima di eseguirli su hardware quantistico reale;
- accedere ad hardware quantistico tramite l'accesso ai computer quantistici di IBM localizzati nei vari data center, nonché hardware da molti altri fornitori;
- utilizzare meccanismi di mitigazione degli errori tramite una varietà di strumenti.

Q# [99]

SDK introdotto inizialmente per il servizio Azure Quantum, è poi diventato agnostico all’hardware e open source. Q# è un linguaggio autonomo che offre un livello di astrazione più alto rispetto agli altri *framework* considerati. È possibile scrivere un programma con un livello di astrazione che non consideri circuiti e q*ubit* ma solo operazioni ed espressioni come in un classico linguaggio di programmazione; è lasciata comunque la possibilità di scrivere programmi a basso livello.

Il seguente diagramma mostra le fasi attraverso le quali un programma quantistico passa dall’idea all’implementazione completa su Azure Quantum, e gli strumenti offerti dal QDK per ogni fase.

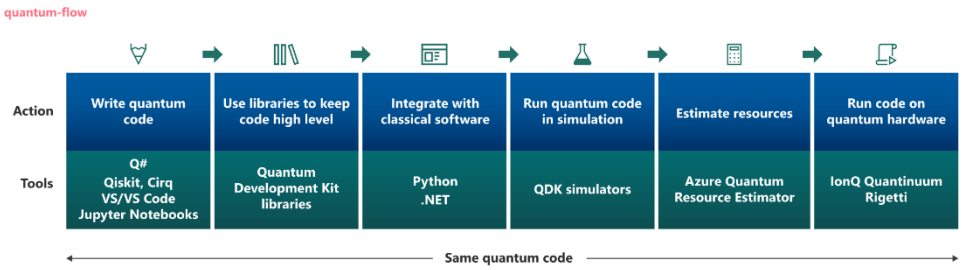


Figura 22 – Diagramma di deploy su Azure Quantum[99]

Oltre a librerie standard, il QDK include anche una libreria di *machine learning* quantistico che fornisce un’implementazione dei classificatori sequenziali che sfruttano il calcolo quantistico per eseguire esperimenti di ML ibridi quantistici/classici.
Una volta creato un Azure Quantum workspace, è possibile inviare i programmi Q# (noti anche come jobs) al servizio cloud Azure Quantum direttamente tramite l’ambiente di sviluppo; il diagramma seguente mostra il processo di rilascio del programma, simile a quanto realizzato con Qiskit.

[98] https://qiskit.org/
[99] https://learn.microsoft.com/it-it/azure/quantum/overview-what-is-qsharp-and-qdk

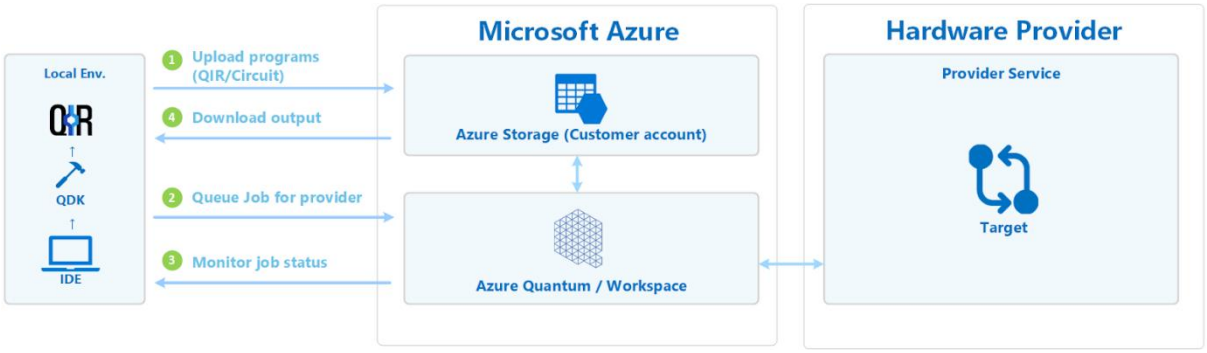


Figura 23 – Ciclo di sviluppo dei programmi nel *framework* Q#[99]

Cirq [100]

Sviluppato da Google AI Quantum si definisce come una libreria Python per scrivere, manipolare e ottimizzare circuiti quantistici ed eseguirli su computer quantistici e simulatori. Nella descrizione è già esplicitato l’approccio, che può essere definito di astrazione a basso livello (*low level control*), di descrizione dei circuiti e gate simile a Qiskit. Cirq include, come gli altri *framework* analizzati, un ambiente di simulazione, però con alcune caratteristiche peculiari, quali la possibilità di lavorare in ambiente noisy e non, in modo da condurre simulazioni realistiche sull’hardware quantistico, o simulazioni idealizzate ai fini di concentrarsi sulla scrittura del programma Python.

Il ciclo di sviluppo è simile a quello visto per gli altri SDK e prevede l’utilizzo di simulatori e la modalità batch per accodare i lavori sul Cloud dove è presente l’Hardware Quantistico.

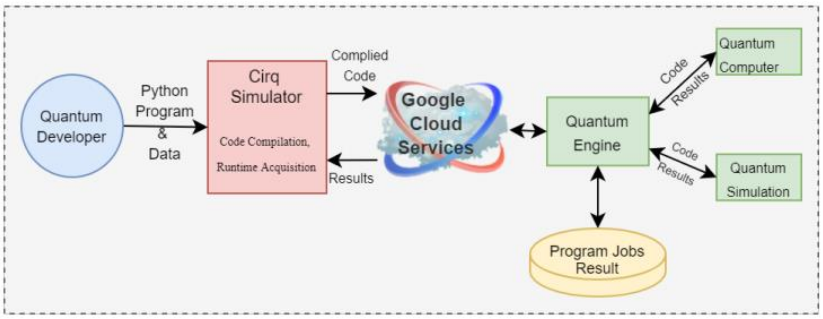


Figura 24 - Ciclo di sviluppo dei programmi nel *framework* Cirq - Source https://arxiv.org/pdf/2302.08884.pdf

La community a supporto di Cirq è più piccola rispetto alle altre analizzate ma un fenomeno che sta diventando sempre più diffuso è la collaborazione tra i vari team di sviluppo per realizzare una compatibilità *cross* (interoperabilità tra *framework*).

4.5.4 QKD

Gli apparati che realizzano la distribuzione di chiavi quantistiche, in generale, sono basati sull’emissione e sul rilevamento di fotoni. Dal punto di vista operativo, essi si integrano nell’infrastruttura tecnologica esistente come gli apparati di cifratura tradizionale che devono essere predisposti per fare uso delle chiavi generate in tal modo.

[100] https://quantumai.google/cirq

Diversi operatori di mercato offrono soluzioni tecnologiche mature per lo scambio di chiavi tramite QKD: si tratta di dispositivi dedicati, con apparati per emissione e ricezione di fotoni le cui caratteristiche sono utilizzate per codificare l’informazione destinata a costituire la chiave. L’offerta di mercato relativa a questi apparati è oramai ampia, variegata e consente una trasmissione con un *key rate* fino a centinaia di Mbps per un range fino a 120 Km. Tuttavia l’introduzione di questi dispositivi comporta costi non indifferenti e una adeguata progettazione dei casi d’uso per garantire performance e affidabilità.

Ci sono vari attori in questo mercato, dai produttori di hardware alle offerte di servizi, ma, data l’estrema novità del tema e la difficoltà a reperire competenze in questo ambito, anche le aziende focalizzate nella produzione di hardware offrono servizi di consulenza, accompagnati da Proof of Concept.

Per l’utilizzo di questi dispositivi è consigliato l’uso di fibra ottica dedicata, ma alcuni di essi funzionano (con prestazioni differenti) anche condividendo la stessa fibra del traffico cifrato. Inoltre, alcuni dispositivi includono la possibilità di usufruire di una componente QRNG per la generazione di chiavi genuinamente stocastiche.

Il mercato è molto vario: da grandi player di mercato (Toshiba) o solide compagnie con questo core business (IDQuantique, Quintessence Lab) a start up (MagiQ, QTI) a spin-off nate da centri di ricerca (Max Planck institute, KETS quantum security – università di Bristol, Ki3 Photonics – Montreal National research center, NuQuantum – Cambridge University). Ci sono anche compagnie focalizzate sull’offerta di servizi via satellite (LevelQuantum).

L’interfaccia verso questi dispositivi per garantire l’accesso alle chiavi simmetriche da parte dei dispositivi cifranti, secondo lo standard ETSI GS QKD 014 (Protocol and data format of REST-based key delivery API) è garantita dai principali produttori (ad esempio: Cisco, Ciena, ecc.).

4.5.5 QRNG

La produzione di strumenti per la generazione di numeri random partendo da sorgenti fisiche che sfruttano i principi della fisica quantistica ha visto un incremento durante gli ultimi quindici anni.

Anche in questo caso si possono individuare diverse aziende che negli anni hanno sviluppato o stanno sviluppando una certa esperienza nello sviluppo di strumenti per la generazione di numeri random. Tra queste troviamo Id Quantique, Quantum Dice, QuintessenceLabs Pty Ltd, Qrypt, Quside, Crypta Labs.

Vengono inoltre proposti strumenti che supportano l’accesso di multiple applicazioni contemporaneamente, e sono particolarmente indicati per le applicazioni di sicurezza o le soluzioni di gaming, dai *data center* ai sistemi in cloud[101].

4.5.6 Servizi di consulenza

La complessità dell’approccio alle tecnologie quantistiche può essere gestita avvalendosi delle numerose società di consulenza presenti sul mercato; sono infatti diversi i servizi di consulenza sorti recentemente, con l’intento di seguire le aziende nell'affrontare le sfide e capitalizzare sulle

[101] Esistono servizi che mettono a disposizione l’accesso tramite API per avere stringhe di numeri casuali realizzate in laboratorio (ad esempio: https://quantumnumbers.anu.edu.au/).

opportunità derivanti dalle tecnologie quantistiche. Il mercato è attualmente molto vivace e, oltre ai grandi player tradizionali, anche aziende di dimensioni più contenute, tra cui numerose start up, stanno proponendo servizi di varia natura.

I servizi di consulenza più comuni, offerti dalla maggior parte delle aziende specializzate, sono i seguenti:

- supporto nell’analisi del rischio quantistico: valutazione di impatto sulle attività aziendali, identificazione delle aree di maggiore vulnerabilità e delle relative opportune azioni di mitigazione coerenti con la strategia aziendale;
- supporto nell’introduzione di misure di mitigazione: sviluppo e introduzione di strategie per la protezione dei dati sensibili, realizzazione di un *crypto inventory*, supporto all’adozione di algoritmi di crittografia post-quantistica, integrazione di soluzioni di sicurezza quantum *resistant* nelle infrastrutture esistenti;
- valutazione delle opportunità di business: supporto all’identificazione di opportunità di business derivanti dalle tecnologie quantistiche, sviluppo di applicazioni e servizi basati su algoritmi quantistici, ottimizzazione dei processi aziendali utilizzando algoritmi quantistici o l'esplorazione di nuovi modelli di business abilitati dalla computazione quantistica;
- formazione e sensibilizzazione: offerta di programmi di formazione e sensibilizzazione per educare il personale aziendale;
- collaborazioni strategiche: interazioni con aziende, istituti di ricerca e fornitori di tecnologia quantistica per l’accesso a risorse specializzate.

5 Quantum *Safety*

La necessità di individuare rapidamente una strategia per la transizione quantum *safe* è espressa in modo molto intuitivo (cfr. Figura 25) da quello che in letteratura viene citato come "teorema di Mosca" (dal suo autore Michele Mosca, prof. nell'University of Waterloo in Canada).

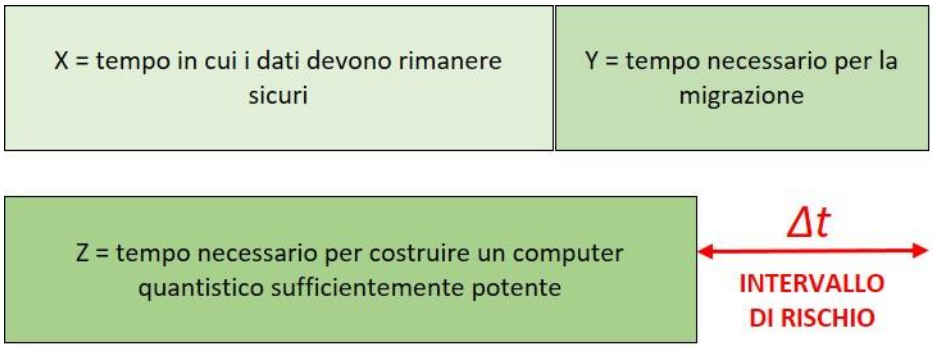


Figura 25 - *Timeline* rappresentativa di una esposizione al rischio compromissione per un tempo Δt se X+Y>Z

Se la somma del tempo per cui i dati devono essere mantenuti sicuri (X) e del tempo necessario per migrare infrastrutture e applicazioni a soluzioni quantum *safe* (Y) è maggiore del tempo (Z) in cui si stima la disponibilità di un computer quantistico capace di violare i sistemi di crittografia moderna allora, per un certo Δ*t*, ci si troverebbe gravemente esposti a un potenziale rischio di compromissione.

Le variabili dipendono fortemente dalle differenti realtà. Ci sono contesti dove, per ragioni legali o di business, i dati devono rimanere confidenziali per decenni (X). La variabile Y, inoltre, è più difficile da stimare, in quanto legata alla complessità dell'infrastruttura ICT sottostante.

Per quanto riguarda la variabile Z, ovvero il tempo necessario allo sviluppo della tecnologia per rappresentare un rischio alla validità di RSA-2048, le stime di esperti, analisti e le roadmap dei produttori convergono, nonostante un margine di incertezza non trascurabile, verso un orizzonte temporale di 20-30 anni[102].

La minaccia riguarda anche le informazioni confidenziali attualmente cifrate in modo ordinario. Un pirata informatico potrebbe aprire un *breach* nei sistemi di archiviazione e conservare i *dataset* sottratti, per decifrarli nel momento in cui la tecnologia risulti matura per farlo. Tale tipo di attacco, denominato *harvest now, decrypt later* è di particolare impatto per tutti quei settori ove vengono gestite quotidianamente e storicizzate informazioni classificate (piani strategici, segreti industriali o ordini militari). Per quanto riguarda nello specifico il mondo finanziario, l'utilizzo della crittografia è pervasivo (Figura 26).

[102] https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

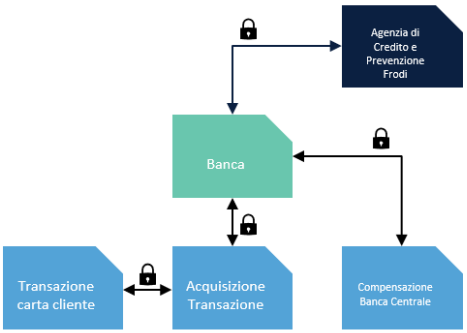


Figura 26 - Utilizzo della crittografia in *use case* tipici dell'ambito bancario e finanziario[103]

In assenza di contromisure adeguate, un attaccante dotato di un computer quantistico sufficientemente potente potrebbe compromettere la sicurezza dei dati personali e transazionali, i sistemi di autenticazione (compresi quelli basati su certificati pur emessi da *Certification Authority* accreditate) degli utenti e delle applicazioni nelle interfacce, i sistemi basati su *Distributed Ledger Technology* (DLT), l'integrità del software, le firme digitali e altro ancora. In particolare, per un istituto bancario anche la compromissione di una firma digitale rappresenta un rischio significativo, in quanto altererebbe la validità di contratti e/o transazioni.

L'attività di definizione di un *Quantum Threat Model* ha proprio come finalità quella di identificare i rischi associati alle vulnerabilità degli attuali algoritmi di cifratura in relazione all'avvento di un computer quantistico. Un *Threat Model* permette di identificare le priorità in termini temporali ed economici anche in relazione ad eventi la cui data di accadimento non è ben definita. Di seguito un esempio di *Quantum Threat Model* presentato da Santander durate il PKI Consortium a Dicembre 2023[104]:

Dimensione	Casi d'uso	Validità nel tempo	Disponibilità esterna	Sensibilità	Rischio
Confidenzialità	Siti pubblici cifrati con TLS	1	5	5	25
	Accesso interno ai server usando SSH	2	1	3	6
	Telelavoro con VPN	3	3	5	45
	VPN da sito a sito usando IPSec	5	3	5	75
	Cifratura dei dati a riposo on-premise (dischi, backup, etc.)	5	2	3	30
	Cifratura dei dati a riposo in cloud	5	3	5	75
Autenticazione	Certificati Digitali Pubblici	2	5	5	50
	Certificati Digitali Interni	2	1	4	8
Apetti legali	Firma digitale dei contratti	5	4	5	100

5.1 Il processo di migrazione ad algoritmi *post quantum*

Una transizione verso sistemi crittografici "post-quantistici" richiede un percorso che passa attraverso alcune fasi fondamentali:

- identificazione di tutti i casi di utilizzo di algoritmi a chiave pubblica nell'hardware, nell'infrastruttura di rete, nei sistemi operativi, nei programmi applicativi, nei protocolli di comunicazione, nelle PKI e nei meccanismi di *access control*;

[103] UK Finance https://www.ukfinance.org.uk/system/files/2023-11/Minimising%20the%20risks%20-%20quantum%20technology%20and%20financial%20services.pdf (pagina 20)

[104] https://www.youtube.com/watch?v=RbwwxZSBjyo

- individuazione delle priorità da assegnare alle componenti per la migrazione, tramite l'uso di un metodo di gestione del rischio.

È possibile trarre spunti da svariati documenti disponibili online, tra cui si segnala il documento NIST 1800-38A "*Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography*". Per un approccio più metodologico ci si può ispirare alle pubblicazioni di diversi enti internazionali: European Telecommunications Standards Institute (ETSI), World Economic Forum (WEF), Cloud Security Alliance (CSA) o Financial Services Information Sharing and Analysis Center (FS-ISAC).

Nella seguente figura è mostrata una comparazione delle diverse metodologie, con una mappatura per colore che identifica fasi simili (source: Santander – PKI Consortium - Dicembre 2023[104]).

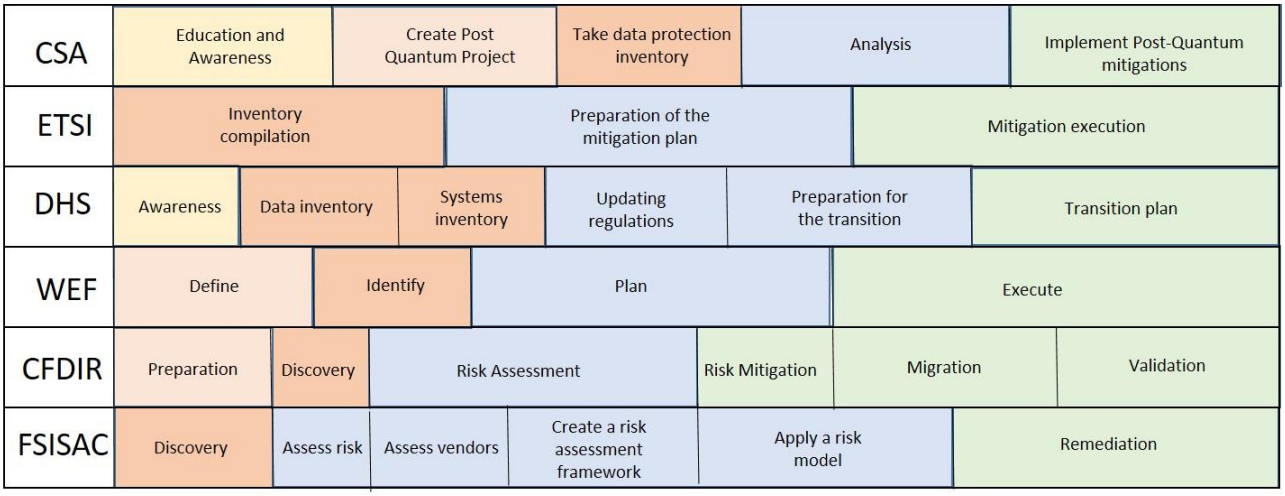


Figura 27 - Comparazione delle diverse metodologie per la transazione quantum *safe*

Il numero di fasi complessive e la sequenza da seguire potrebbe variare in base alle dimensioni dell'organizzazione, alle attività pregresse o alla metodologia a cui si fa riferimento.

In riferimento a quella descritta dal World Economic Forum[105], e aggiungendo una fase iniziale di *awareness*, si suggerisce di identificare cinque macro-fasi di un ipotetico piano di migrazione:

- *awareness* (o *education*): coinvolgento del management nella consapevolezza dei rischi associati a una gestione tardiva della problematica;
- *define* (o *preparation*): definizione di obiettivi, strategia, costruzione di una *roadmap*, stima del budget necessario, creazione del gruppo di lavoro nonché individuazione di aspettative sul breve, medio e lungo termine;
- *identify* (o *discovery*): identificazione degli ambiti dove vengono utilizzati algoritmi di cifratura (applicazioni, hardware e servizi) sia internamente all'azienda sia dalle terze parti. Lo scopo primario è quello di costruire un inventario crittografico (*crypto inventory*) interrogabile e aggiornato che permetta di indentificare dove intervenire e con quali impatti, nel caso sia necessario sostituire una metodologia di cifratura utilizzata;

[105] https://www.weforum.org/publications/quantum-economy-blueprint/

- *plan* (o *analysis/risk assessment*): pianificazione degli interventi in linea con un *Quantum Threat Model* finalizzato ad assegnare le priorità di intervento. È fondamentale considerare il tempo di vita del dato (ad esempio potrebbe non essere necessario proteggere un contratto con validità annuale rispetto a uno con validità decennale);
- *execute* (o *mitigate/remediate*): esecuzione delle attività: dall'utilizzo di logiche ibride (PKI con certificati che contengono sia un algoritmo tradizionale, come RSA, sia un algoritmo resistente a un attacco quantistico come Dilithium) all'utilizzo di logiche interamente post-quantum.

Nel capitolo 8.2 è riportata una descrizione più dettagliata di queste azioni.

Di seguito un altro esempio di piano di migrazione, di diversa impostazione ma sempre comprensivo di riferimenti temporali, tratto dal documento del 2021 "Canadian National Quantum – Readiness"[106]. Sono previste due macrofasi (cfr. Figura 28):

1. pianificazione / scopo: comprende una preparazione, *discovery* e *risk assessment* / *analysis* partendo da una *Business Impact Analysis* si potrebbe dare una priorità ai processi core / sistemici, gestendo gli altri in ondate successive.
2. implementazione: comprende la mitigazione dei rischi, una migrazione verso sistemi quantum *safe* e una validazione di quanto implementato.

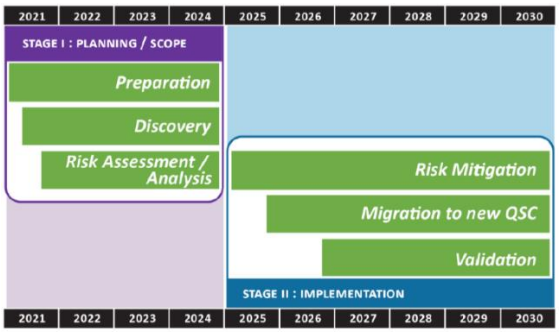


Figura 28 – Esempio di pianificazione delle macrofasi[106]

La finalità ultima di un'attività di migrazione verso una cifratura quantum *safe* è quella di giungere a un'implementazione agile (*crypto agility*) che permetta di adattarsi all'evoluzione di un contesto informatico, per sua natura fortemente dinamico e scarsamente prevedibile e che consenta di adeguare facilmente le proprie soluzioni IT ad ulteriori aggiornamenti (come ad esempio nuovi standard di cifratura).

5.2 *Crypto Agility*

Il processo di selezione avviato dal NIST ha prodotto, tra le altre cose, una intensa competizione tra critto analisti di tutto il mondo che hanno concentrato gli sforzi nell'individuare vulnerabilità nei vari algoritmi candidati a sostituire quelli su cui si basano i protocolli crittografici a chiave pubblica oggi largamente impiegati. Sono in corso ulteriori test per valutare l'effettiva sicurezza crittografica di

[106] https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf

ciascuno di questi algoritmi rispetto agli attacchi possibili, misurarne le rispettive performance e sviluppare tecniche di implementazione sicura. E' ragionevole aspettarsi che tale lavoro continuerà anche nei prossimi anni anche in considerazione del fatto che nuove tecniche computazionali e nuovi approcci potrebbero mostrare come vulnerabili algoritmi crittografici che oggi sembrano sicuri. In quest'ottica, algoritmi come Crystals-Kyber, Falcon, SPHINCS+ non vanno intesi come i sostituti definitivi di RSA o ECC (*Elliptic Curve Cryptography*) ma come prime soluzioni quantum-*resistant* al momento disponibili, le quali potranno a loro volta essere abbandonate in favore di algoritmi più performanti o più robusti.

Pertanto, è necessario non vincolarsi a uno specifico algoritmo, bensì predisporre i propri sistemi in modo tale da renderli indipendenti dalla componente utilizzata. Molti dei sistemi informatici in uso non sono progettati per favorire un rapido adattamento di nuove primitive e algoritmi crittografici senza apportare modifiche significative all'intera infrastruttura del sistema. L'esperienza di rimozione di funzioni di *hashing* oggi deprecate, come MD5 o SHA-1, ha evidenziato come una migrazione crittografica può risultare difficile e onerosa in termini di risorse. La stessa NSA ha dichiarato come la migrazione alle nuove logiche crittografiche potrebbe richiedere al sistema di sicurezza nazionale americano fino a 20 anni[107].

Si definisce *crypto agility* è la capacità di reagire velocemente alle minacce crittografiche, sostituendo gli algoritmi crittografici diventati vulnerabili in modo che l'impatto sulle infrastrutture coinvolte e sulla continuità di business sia il minimo possibile.

L'implementazione della *crypto agility* richiede un disaccoppiamento tra le logiche di cifratura e le logiche di sviluppo del codice, in modo tale che la gestione sia esterna all'applicativo stesso.

Di seguito sono elencati alcuni dei benefici che la *crypto agility* può introdurre:

- utilizzare alternativamente, a rotazione, diversi algoritmi di cifratura senza modificare il codice applicativo o l'infrastruttura;
- consentire una rapida transizione da un algoritmo di cifratura a un altro (nel caso occorra mitigare delle nuove vulnerabilità su algoritmi esistenti);
- consentire una implementazione ibrida dove possono convivere algoritmi classici e algoritmi post-quantum;
- consentire la decisione sul tipo di cifratura da utilizzare agli esperti di sicurezza in base alla classificazione del dato o alle policy interne;
- astrarre le API, ovvero nascondere la complessità della cifratura agli sviluppatori delle applicazioni;
- supportare il maggior numero di piattaforme possibili (inteso come linguaggi di programmazione differenti e/o tecnologie differenti, come ad esempio i *containers*);
- interoperare facilmente con sistemi che utilizzano implementazioni crittografiche diverse;

[107] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

- adeguarsi a nuovi standard normativi, senza impatti sostanziali e minimizzando il lavoro richiesto.

Alcuni *vendor,* molti dei quali membri del consorzio cooperativo sul quantum che fa capo al NIST[108], si sono già affacciati sul mercato con soluzioni che permettono l'implementazione di un *framework* di *crypto agility*. Altri fornitori propongono invece una *crypto agility* nativamente *embedded* nei prodotti/servizi proposti, facilitando così l'aggiornamento a nuovi standard/protocolli/algoritmi (es. Crypto4A, CryptoNext, DigiCert, Thales).

E' anche possibile implementare la *crypto agility* attraverso specifiche *features* offerte da alcuni linguaggi di programmazione, senza dover necessariamente ricorrere a strumenti di terze parti. Ad esempio, le Cryptography API Next Generation (CNG) – in sostituzione delle CryptoAPI – sono fornite con metadati di crittografia che permettono di identificare immediatamente la tecnica crittografica utilizzata e sostituire le funzioni crittografiche tramite riconfigurazione o patch. *Features* già presenti in .NET, Java Cryptography Architecture (JCA), Node.js, Ruby o Go and Python permettono di realizzare software nativamente critto-agili.

Il punto nevralgico dove implementare i controlli necessari per evitare implementazioni non critto-agili è la catena DevOps. Integrandosi con le catene esistenti, in logica CI/CD (integrazione continua/distribuzione continua), si può permettere agli sviluppatori di accedere a linee guida conformi alle policy. È buona prassi includere l'implementazione delle modalità di sostituzione dei protocolli di sicurezza all'interno del test book di riferimento, al fine di verificare che esse siano adeguate rispetto ai requisiti di confidenzialità, integrità e disponibilità adottati.

Infine, nel mondo IoT, l'approccio alla *crypto agility* potrebbe rivelarsi più complesso. Uno degli scenari implementativi adottabili per minimizzare l'aggiornamento consiste nell'utilizzo di strumenti in grado di ricevere allo stesso modo chiavi, nuovi algoritmi di cifratura e policy di sicurezza da implementare localmente. Un'implementazione basata su firmware ha come lato negativo il necessario riavvio del dispositivo con un possibile impatto in termini di disservizi se il dispositivo diventasse, per qualche motivo, irraggiungibile. Poter aggiornare dinamicamente un algoritmo di cifratura ridurrebbe sensibilmente questo rischio.

5.3 Adozione di scenari QKD

Nell'adozione di questa tecnologia vanno considerate alcune limitazioni, che molti attori, anche istituzionali, hanno già evidenziato (con relativo dibattito[109]) e che possono essere sintetizzate nei seguenti aspetti:

- costi legati agli apparati necessari per la generazione e la distribuzione di chiavi quantistiche;
- limitata distanza della connessione punto punto a causa della dispersione a cui è soggetto il mezzo fisico impiegato per comunicare (es. fibra ottica) in assenza di tecnologie diffuse consolidate per i nodi intermedi di trasmissione;

[108] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

[109] "The debate over QKD: A rebuttal to the NSA's objections" - Renato Renner, Ramona Wolf - https://arxiv.org/pdf/2307.15116

- necessità di affidarsi a meccanismi classici (*pre-shared keys* o crittografia post-quantum), per l'autenticazione iniziale;
- aumentato rischio di attacchi di tipo DoS (Denial of Service) a causa dell'elevata sensibilità alle interferenze del protocollo.

Inoltre, è necessario considerare che, per quanto gli apparati QKD siano disponibili sul mercato da diverso tempo e con un grado di maturità elevato, gli standard per il loro funzionamento, la valutazione delle loro performance, nonché il grado di interoperabilità con altri dispositivi rappresentano ancora elementi di analisi nell'introduzione di questi scenari.

6 Le tecnologie quantistiche e il settore bancario e finanziario

6.1 Sfruttare le opportunità del quantum *computing* nelle applicazioni finanziarie

Si stima[110] che quello dei servizi finanziari sia il primo settore industriale che trarrà beneficio dal calcolo quantistico nel medio e lungo periodo. La lista degli *use case* utili è lunga ma molti di essi fanno riferimento spesso agli stessi algoritmi fondamentali che vengono riutilizzati in più contesti. (Figura 29).

Author(s)	Year	Title	Use Case	Methodology	Quantum algorithm	Hardware
Rebentrost and Lloyd	2018	Quantum computational finance: quantum algorithm for portfolio optimization	Determine the optimal portfolio more quickly/accurately.	Optimisation	Solving linear equation systems (HHL)	Gate-based quantum computer
Venturelli and Kondratyev	2019	Reverse Quantum Annealing Approach to Portfolio Optimization Problems	Determine the optimal portfolio more quickly/accurately.	Optimisation	Approximate optimization (QUBO)	Quantum annealer
Braine *et al.*	2021	Quantum algorithms for mixed binary optimization applied to transaction settlement	Settle as many transactions as possible and/or maximise the total value of the settled transactions.	Optimisation	Approximate optimization (VQE and QAOA)	Gate-based quantum computer
Phillipson and Bhatia	2020	Portfolio Optimisation Using the D-Wave Quantum Annealer	Determine the optimal portfolio more quickly/accurately.	Optimisation	Approximate optimization (QUBO)	Quantum annealer
Y. Ding *et al.*	2019	Towards Prediction of Financial Crashes with a D-Wave Quantum Computer	Prediction of financial crashes in a complex financial network.	Optimisation	Approximate optimization (QUBO adapted)	Quantum annealer
Hodson *et al.*	2019	Portfolio Rebalancing Experiments using the Quantum Alternating Operator Ansatz	More quickly/accurately discrete portfolio optimisation under constraints.	Optimisation	Approximate optimization (QAOA)	Gate-based quantum computer
Kerenidis *et al.*	2019	Quantum Algorithms for Portfolio Optimization	More quickly/accurately portfolio optimisation under constraints.	Optimisation	Optimization (QIPM for SOCPs)	Gate-based quantum computer
Orús *et al.*	2019	Forecasting financial crashes with quantum computing	Forecasting financial crashes with quantum computing.	Optimisation	Approximate optimization (QUBO)	Quantum annealer
Rebentrost *et al.*	2018	Quantum Computational Finance: Monte Carlo Pricing of Financial Derivatives	Price derivatives more quickly/accurately	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer
Martin *et al.*	2021	Toward pricing financial derivatives with an ibm quantum computer	Pricing interest-rate financial derivatives with the Heath-Jarrow-Morton model more quickly	Monte Carlo	Optimization (qPCA)	Gate-based quantum computer
Egger *et al.*	2019	Credit Risk Analysis using Quantum Computers	Estimate credit risk more efficiently.	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer
Woerner and Egger	2019	Quantum Risk Analysis	Evaluate risk measures such as Value at Risk and Conditional Value at Risk more quickly/accurately	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer
Stamatopoulos *et al.*	2020	Option Pricing using Quantum Computers	Price options such as vanilla options, multi-asset options, barrier options and path-dependent options more quickly/accurately	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer

Figura 29 – Panoramica di casi d'uso proposti in letteratura nell'ambito finanziario[111]

[110] Il Quantum Technology Monitor 2023 di McKinsey stima che i quattro settori (automobilistico, prodotti chimici, servizi finanziari e scienze della vita) che vedranno i primi benefici dell'uso del calcolo quantistico potrebbero guadagnare potenzialmente fino a 1,3 miliardi di dollari entro il 2035. Di questi, la metà potrebbe essere appannaggio del settore finanziario.

[111] A Structured Survey of Quantum Computing for the Financial Industry- Albareti et *al.* - 2022 - https://arxiv.org/pdf/2204.10026

Le possibili applicazioni del calcolo quantistico in ambito finanziario possono essere tre macrogruppi[112]:

- problemi di ottimizzazione: ottimizzazione del portafoglio, *credit scoring*;
- problemi di simulazione o modellazione stocastica: simulazione dell'andamento degli asset finanziari, scenari di stress test, previsioni crisi finanziarie;
- apprendimento automatico (*machine learning*): algoritmi di *fraud detection*, personalizzazione dell'offerta al cliente finale.

Nel seguito si fa un breve cenno a queste applicazioni, rimandando alla vasta letteratura scientifica in merito[112] per eventuali approfondimenti.

6.1.1.1 Problemi di ottimizzazione

L'ottimizzazione è il processo di trovare soluzioni che massimizzano o minimizzano una determinata funzione. Tale processo può risultare computazionalmente oneroso in presenza di un numero elevato di variabili da considerare. Questo tipo di problema si presenta in molte aree, quali la finanza, l'arbitraggio o il credito.

La tecnologia quantistica offre nuove possibilità per affrontare i problemi di ottimizzazione combinatoria e convessa, che sono tra i più complessi. Esistono diversi approcci basati sul quantum *computing*, come gli algoritmi adiabatici, variazionali o ibridi, che sfruttano le proprietà dei sistemi quantistici per esplorare lo spazio delle soluzioni (si veda il box sottostante per un esempio).

Il modello QUBO (Quadratic Unconstrained Binary Optimization)

QUBO è un modello utile a risolvere una classe di problemi di natura combinatoria. In questo tipo di problemi sono normalmente presenti una serie di variabili binarie la cui combinazione può rappresentare, a seconda del problema, una perdita o un guadagno. In termini molto semplici, QUBO è caratterizzato da una funzione matematica quadratica da minimizzare in funzione di un set di variabili che tenga conto anche dei vincoli.

Si tratta di un modello molto apprezzato per la sua flessibilità e la capacità di sintetizzare molte variabili in modo efficiente: esso trova applicazione in molti scenari che interessano in particolare il mondo bancario e finanziario[112] come la stima dei *collateral*, l'ottimizzazione del portafoglio, la gestione dell'arbitraggio ma anche altri ambiti come la pianificazione di interventi di manutenzione[113] oppure l'ottimizzazione dell'infrastruttura di reti mobili[114].

La possibilità di sfruttare il parallelismo quantistico consentirebbe di velocizzare e rendere più precisa la sua risoluzione. Lo sviluppo di un algoritmo quantistico QUBO consiste nella formulazione del problema secondo questo modello e nell'utilizzo delle librerie che consentano di risolverlo.

112 A Survey of Quantum Computing for Finance – Herman *et al.* - https://arxiv.org/pdf/2201.02773

113 https://www.reply.com/data-reply/it/stories/algoritmi-quantistici-per-l-ottimizzazione-dei-lavori-di-manutenzione

114 https://www.gruppotim.it/content/dam/telecomitalia/it/archivio/documenti/Innovazione/MnisitoNotiziario/2020/2020-1/cap02_quantum-ottimizzazione.pdf

Anche nei comuni SDK di interfaccia all'hardware quantistico sono stati integrati *solver* di risoluzione per il QUBO. In particolare, i quantum *annealer* sono particolarmente adatti a tale scopo.

6.1.1.2 Problemi di simulazione e modellazione stocastica

La simulazione è una tecnica utile per modellare fenomeni complessi. In ambito finanziario, questa tecnica può supportare le decisioni di investimento, ottimizzando il rapporto tra rendimento e rischio, e facilitare la gestione operativa delle banche in diversi settori, come quello creditizio o quello dei derivati. Anche la modellizzazione di scenari di stress test, accantonamenti di liquidità e previsioni di crisi finanziarie sono ambiti dove potrebbero essere individuati consistenti vantaggi dall'applicazione di questa tecnica. Inoltre, la simulazione può essere di ausilio per le banche al fine di rispettare i requisiti normativi previsti dagli accordi internazionali, come l'accordo Basilea III, che richiede il calcolo di indicatori di rischio quali il Value at Risk (VaR) e il Conditional Value at Risk (CVaR).

Per modellare i processi stocastici che determinano l'evoluzione dei fenomeni finanziari, si usano equazioni differenziali stocastiche, che in genere non hanno una soluzione analitica, ma richiedono metodi numerici o di tipo Monte Carlo[115]. Il quantum *computing*[112] offre nuove possibilità per affrontare questi problemi, con algoritmi che sfruttano le proprietà quantistiche per risolvere equazioni differenziali parziali (QPDE - *Quantum Partial Differential Equations*) o effettuare integrazioni Monte Carlo (QMCI - *Quantum Monte Carlo Integration*). Queste varianti quantistiche offrono un vantaggio computazionale rilevante[116] rispetto agli equivalenti metodi classici.

6.1.1.3 Machine Learning

L'apprendimento automatico è una tecnologia di analisi e previsione che ha trovato molte applicazioni in diversi settori industriali. L'intelligenza artificiale – sia discriminativa, sia generativa – sta cambiando il modo in cui si elaborano le grandi quantità di informazioni disponibili per facilitare le decisioni.

Una prospettiva innovativa è offerta dal quantum *machine learning* (QML, cfr. 3.2.2), che sebbene sia ancora una disciplina emergente e in fase di valutazione scientifica, può presentare vantaggi in alcuni scenari di applicazione. Le aree di ricerca più attive che si avvalgono del QML sono: *asset pricing*, stima della volatilità implicita, *forecasting* di opzioni con *payoff* discontinuo, *credit scoring*

[115] L'idea alla base del metodo Monte Carlo, che comprende in realtà una vasta categoria di tecniche comunemente utilizzate per la stima dei prezzi e la previsione dei rischi, è utilizzare numeri casuali per effettuare simulazioni statistiche di processo che si vuole studiare. Con una estrema semplificazione, l'andamento del particolare processo viene descritto da una espressione matematica in funzione di una variabile dipendente x (la soluzione che si cerca) e di differenti parametri per i cui valori si ipotizzano delle distribuzioni di probabilità (per esempio sulla base di dati storici). Si effettua, quindi, il campionamento di queste distribuzioni generando una serie di valori per ciascuno dei parametri e, iterando il procedimento con le varie combinazioni possibili, si calcolano le rispettive soluzioni con la relativa stima di probabilità e definiti margini di errore. L'attendibilità della stima è legata al numero di ripetizioni del procedimento; di conseguenza, il consumo di risorse e il tempo richiesti per ottenere una stima con il desiderato grado di precisione risultano elevati.

[116] Esistono numerosi paper sul tema, per esempio: "Quantum computational finance: Monte Carlo pricing of financial derivatives"- Rebentrost *et al.* - Physical Review A 30 April 2018 - https://arxiv.org/abs/1805.00109

e stima del cambio di regime dei tassi di cambio. In tutti questi ambiti, la capacità di fare previsioni accurate, tipica degli algoritmi di ML, è di fondamentale importanza.

I principali vantaggi del QML sono legati alla maggiore velocità di training degli algoritmi e alla maggiore precisione nelle simulazioni probabilistiche.

6.2 Rendere sicuri sistemi, applicazioni e infrastrutture

6.2.1 Rendere sicuri i sistemi e le applicazioni

Come descritto diffusamente nel capitolo 5, uno degli aspetti principali, che coinvolge le prime fasi del processo di transizione, è acquisire consapevolezza del proprio parco applicativo e infrastrutturale.

Una distinzione di fondamentale importanza consiste nell'individuare le applicazioni realizzate in casa e quelle oggetto di acquisizione da fornitori esterni delle quali, normalmente, non si conoscono i dettagli del codice di sviluppo e si demandano gli aspetti di sicurezza alle garanzie offerte dagli sviluppatori del prodotto.

6.2.1.1 Le applicazioni sviluppate "in house"

In questo scenario sono fondamentali due aspetti: per prima cosa, la conoscenza di quali algoritmi vengano utilizzati e, in secondo luogo, la predisposizione di un *framework* di sviluppo applicativo che consenta una facile sostituzione di queste variabili.

Può essere utile, inoltre, utilizzare librerie, protocolli e applicazioni già predisposti per valutare il costo e le funzionalità di tali sostituzioni.

Si segnala, a tal proposito, il progetto open-source "Open Quantum Safe"[117] parte del Linux Foundation's Post-Quantum Cryptography Alliance. Il progetto prevede sia lo sviluppo di librerie per algoritmi post-quantum (liboqs), sia l'integrazione in prototipi di applicazioni e protocolli[118].

6.2.1.2 I prodotti commerciali

È bene valutare, nell'adozione di prodotti commerciali corrente e futura, la predisposizione nella *roadmap* del fornitore di meccanismi di *crypto agility*. Questa accortezza diventa di particolare rilievo laddove l'utilizzo della crittografia sia dedicato allo scambio di informazioni sensibili, a transazioni finanziarie, all'autenticazione o, addirittura, all'emissione di certificati digitali.

6.2.1.3 L'ambiente mainframe

In ambito mainframe, tradizionalmente presente nei *data center* delle banche, ci si avvia a una nuova generazione di hardware nativamente predisposta per l'utilizzo di protocolli post-quantum. In particolare, ne è un buon precursore l'IBM z16, il cui firmware è programmabile per poter, attraverso specifici aggiornamenti, provvedere alla sostituzione in modo agile degli algoritmi di cifratura.

[117] https://openquantumsafe.org/

[118] https://openquantumsafe.org/applications/

6.2.2 Rendere sicure le infrastrutture

La possibilità, offerta dalla QKD, di scambiare chiavi in modo sicuro e garantire una cifratura che salvaguardi i dati da compromissioni nell'era post-quantum, può essere sfruttata già da ora nelle comunicazioni di rete.

6.2.2.1 Rendere sicure le comunicazioni *peer-to-peer* tra *data center*

Il caso d'uso più semplice, ma che caratterizza molti dei *data center* IT è quello che riguarda la connessione tra due siti che sono, solitamente, presenti negli ambienti ridondati tipici delle infrastrutture critiche e a distanza relativamente breve (dell'ordine dei 50-100 Km per consentire l'efficiente replica sincrona dei dati).

Normalmente, l'infrastruttura di rete che connette i due siti è costituita da canali in fibra ottica ove i dati transitano cifrati grazie ad apparati (cifratori) che utilizzano protocolli simmetrici, come AES, considerati quantum *safe*. Tuttavia, la chiave utilizzata a tale scopo è scambiata, dagli stessi cifratori, tramite lo stesso canale, utilizzando un protocollo asimmetrico.

La vulnerabilità del sistema ad attacchi condotti con elaboratori quantistici è individuabile proprio in questo scambio (cfr. Figura 30).

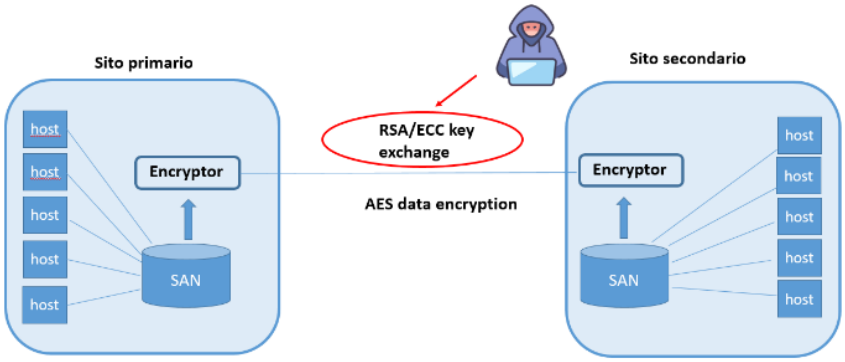


Figura 30 – Vulnerabilità delle connessioni intra data center

Per rendere quantum *safe* questa connessione è necessario:

- introdurre apparati ottici per lo scambio delle chiavi;
- collegarli tramite una fibra ottica dedicata[119];
- configurare i dispositivi crittografici per utilizzare le chiavi generate dagli apparati ottici (Figura 31).

[119] È possibile utilizzare anche una fibra condivisa, utilizzando tecniche di multiplexing ma le interferenze presenti potrebbero ridurre l'efficienza nella creazione delle chiavi.

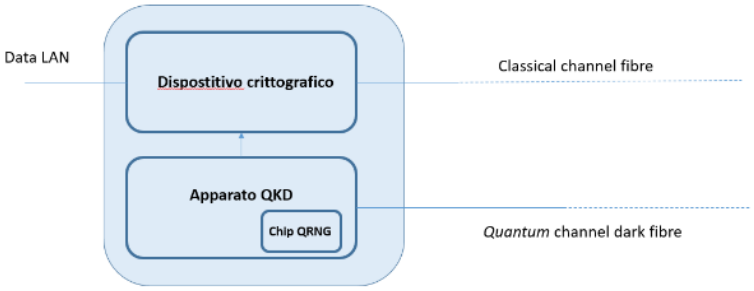


Figura 31 – Schema logico di endpoint per lo scambio QKD

Lo schema di una connessione data center quantum safe è descritta nella figura seguente:

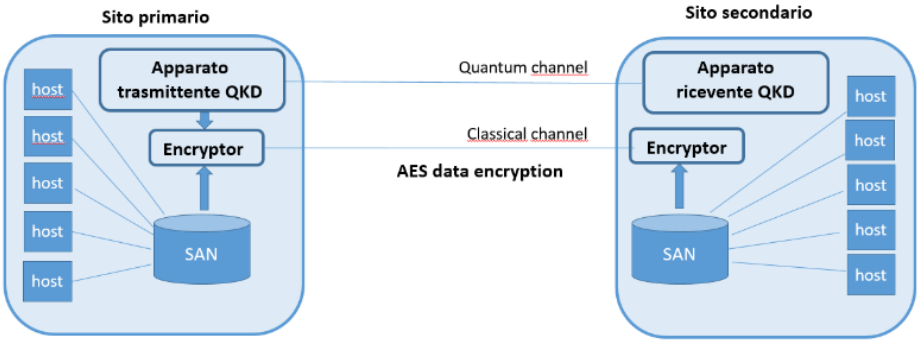


Figura 32 – Infrastruttura data center *quantum safe*

6.2.2.2 I prestatori di servizi fiduciari attivi di firma elettronica certificata

Anche i sistemi accreditati di emissione di certificati per la cifratura e la firma sono, per ovvie ragioni, esposti alle minacce quantistiche. In particolare, la firma elettronica qualificata, sulla quale si basa l'attendibilità di molti documenti conservati digitalmente, richiede particolare attenzione per il fatto che la sua validità viene richiesta nel tempo. Tra i fornitori di questo servizio in Italia, oltre alla Banca d'Italia, sono presenti varie entità bancarie e finanziarie.

Per questo motivo, i produttori di tecnologia e soluzioni per infrastrutture a chiave pubblica (PKI) hanno già inserito, nella loro *roadmap*, indicazioni per l'adozione di algoritmi post-quantum e sperimentazioni possono essere introdotte anche sfruttando il software open source[120].

6.2.2.3 Quantum DLT

La tecnologia a registro distribuito basa la sua stessa esistenza sulla crittografia e, in particolare, sull'utilizzo di chiavi per la cifratura e la firma.

Le criptovalute sono una delle principali applicazioni di questa tecnologia dove le coppie di chiavi pubbliche e private sono utilizzate per mantenere gli indirizzi e le firme per siglare le transazioni.

[120] https://www.ejbca.org/use-cases/try-quantum-safe-cryptography-pki/

Alcuni degli attuali network di blockchain hanno dichiarato[121] di avere in corso studi e sperimentazioni per rendere l'infrastruttura *quantum resistant*.

La QKD, in linea di principio, potrebbe essere utilizzata per rendere sicure le transazioni effettuate tramite le tecnologie distribuite ma gli approcci risultano, al momento, alquanto onerosi sia per la difficoltà a ipotizzare che tutti i partecipanti alla DLT abbiano a disposizione un collegamento (via fibra o satellite) per realizzare lo scambio di chiavi quantistiche, sia perché il bit-rate attuale potrebbe comprometterne la performance.

In alternativa, è ipotizzabile il passaggio ad algoritmi post-quantum (PQC) anche se le attuali implementazioni degli algoritmi di firma digitale e di cifratura (es. Crystal Dilithium e Kyber) appaiono ancora immature.

Diversi operatori sul mercato offrono soluzioni per rendere quantum *safe* le applicazioni basate su DLT: QuantiCor Security e QANPlatform, Sonora Gold and Silver Corp (PQC), Quantum Blockchain o entrambe (QuSecure).

6.3 Esperienze del settore bancario e finanziario

Di seguito sono riportare alcune esperienze, ufficialmente rese note e ritenute significative, del panorama bancario e finanziario internazionale.

I dati che accomunano queste esperienze possono essere sintetizzati come segue:

- nella maggior parte dei progetti sono stati introdotti accordi di collaborazione con l'industria rappresentata sia dai grandi *vendor* (che spesso offrono un servizio comprensivo di una fase di apprendimento, del software, della disponibilità dell'hardware e del supporto allo sviluppo) sia da start up che propongono servizi specifici; la strategia di alcuni gruppi bancari è caratterizzata dall'investimento diretto in start up ritenute promettenti;
- alcuni istituti hanno individuato collaborazioni con il mondo accademico e della ricerca, in particolare per lo studio, applicazione e miglioramento di algoritmi esistenti; tali collaborazioni hanno come risultato la pubblicazione congiunta di articoli scientifici;
- le sperimentazioni vere e proprie sono generalmente precedute da una fase piuttosto lunga di apprendimento e da una di analisi di *use case* di particolare interesse per il business per i quali la soluzione classica non è efficiente o è limitata nell'uso dei parametri come, ad esempio, l'ottimizzazione della stima del rischio di credito (*credit scoring*), individuazione delle frodi (*fraud detection*) oppure l'ottimizzazione del portafoglio;
- alcuni istituti stanno creando team dedicati, avvalendosi di formazione interna ed esterna, per seguire le evoluzioni della tecnologia e individuare rapidamente strategie di migrazione;

[121] "Future proofing - Quantum resistant" https://ethereum.org/en/roadmap/future-proofing/, "Pioneering falcon post quantum technology on blockchain" (https://www.algorand.foundation/news/pioneering-falcon-post-quantum-technology-on-blockchain)

- per quanto riguarda la componente relativa alla quantum network security, risulta inevitabile la collaborazione con enti di ricerca e provider di infrastrutture di rete per la realizzazione di progetti di collegamento;
- seppur con importanti eccezioni, molte delle realtà commerciali che hanno investito sul tema delle tecnologie quantistiche, non hanno ufficialmente dichiarato progetti di grande rilievo per l'introduzione di contromisure quantum *safe*; questo tipo di indagine è invece promossa da istituzioni come la Banca d'Italia, diverse altre banche centrali, ABI e Bank for International Settlement (BIS) che hanno avviato diverse iniziative al loro interno e per sensibilizzare l'intero sistema all'importanza di adeguare per tempo applicazioni e infrastrutture;
- in generale, per quanto riguarda il tema della transizione *quantum safe*, i singoli istituti tendono, per la natura del tema, a manifestare un approccio condiviso in consorzi o iniziative e indicazioni promosse dalle istituzioni.

6.3.1 Banca d'Italia

La Banca d'Italia ha avviato da tempo un percorso di approfondimento delle tecnologie quantistiche che vede coinvolti i Dipartimenti Informatica ed Economia e Statistica.

A una fase di studio, che ha visto la pubblicazione di specifici paper all'interno delle collane dell'Istituto[122], la partecipazione come relatori a eventi internazionali e l'organizzazione di un workshop dedicato con la partecipazione del mondo accademico, sono seguite delle fasi di sperimentazioni, tuttora in corso, finalizzate ad aumentare le conoscenze e sensibilizzare verso opportunità e rischi in questo ambito.

Figura 33 – Pubblicazioni della Banca d'Italia su temi legati alle tecnologie quantistiche

122 Elena Bucciol e Pietro Tiberi "Quantum safe payment systems" June 2023 - https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2023-035/index.html

Giuseppe Bruno "Quantum computing: a bubble ready to burst or a looming breakthrough?" October 2022 - https://www.bancaditalia.it/pubblicazioni/qef/2022-0716/index.html

Adriano Baldeschi e Giuseppe Bruno "Quantum Computing winks at statistics. Is it a good match?" April 2024 - https://www.bancaditalia.it/pubblicazioni/qef/2024-0843/index.html

In particolare, tali sperimentazioni sono state relative a:

- ricognizione dei sistemi e del patrimonio applicativo per l'utilizzo degli algoritmi quantum *safe*;
- possibilità di sfruttare apparati QKD per scambio di chiavi in modo sicuro tra i *data center* e realizzazione di collegamenti sicuri internazionali;
- sperimentazione di *Certification Authority* (CA) con l'uso di software predisposto per l'utilizzo degli algoritmi *post* quantum.

Per quanto riguarda il primo aspetto, in linea con le indicazioni strategiche descritte anche nel presente rendiconto, è stata preliminarmente condotta una analisi di mercato dell'offerta software per individuare una soluzione idonea a identificare e catalogare gli algoritmi di crittografia utilizzati dalle numerose applicazioni sviluppate all'interno dell'Istituto. Tali informazioni verranno integrate all'interno del *repository* degli asset applicativi già in uso per costituire una base informativa sulla quale pianificare priorità e modalità di intervento in ottica di *crypto agility*.

Con riferimento al secondo aspetto, è stata sperimentata la connessione dati cifrata tra tre *data center* (con distanza compresa tra 10 e 20 Km) utilizzando chiavi generate attraverso apparati ottici per lo scambio di chiavi quantistico (QKD). A tale scopo è stata configurata un'interfaccia tra questi ultimi e i dispositivi di cifratura di vari *vendor,* consentendo di valutare requisiti di efficienza (in termini di *key rate*), affidabilità e interoperabilità. L'esperienza è stata di grande valore per valutare lo sforzo e l'impatto richiesto per realizzare un'infrastruttura di questo tipo.

Grazie alla collaborazione con la Bank of Canada e con la Banque de France è stato possibile realizzare dei collegamenti sicuri tramite l'utilizzo di un protocollo[123] basato sulla crittografia simmetrica per lo scambio delle chiavi di cifratura.

[123] " Distributed Symmetric Key Exchange: a scalable, quantum-proof key distribution system"- Hoi-Kwong Lo, Mattia Montagna, Manfred von Willich - https://arxiv.org/abs/2205.00615. Questo meccanismo prevede l'introduzione di *security hu*b ai quali si rivolgono i client per negoziare una chiave simmetrica per comunicare tra loro. Il metodo prevede una fase iniziale di scambio (con ciascun *security hub* presente) di un certo quantitativo di stringhe random (generate tramite QRNG) *pre-shared*, consegnate fisicamente oppure distribuito tramite QKD (gli autori immaginano una rete di distributori locali che faciliti la trasmissione fisica o tramite QKD).

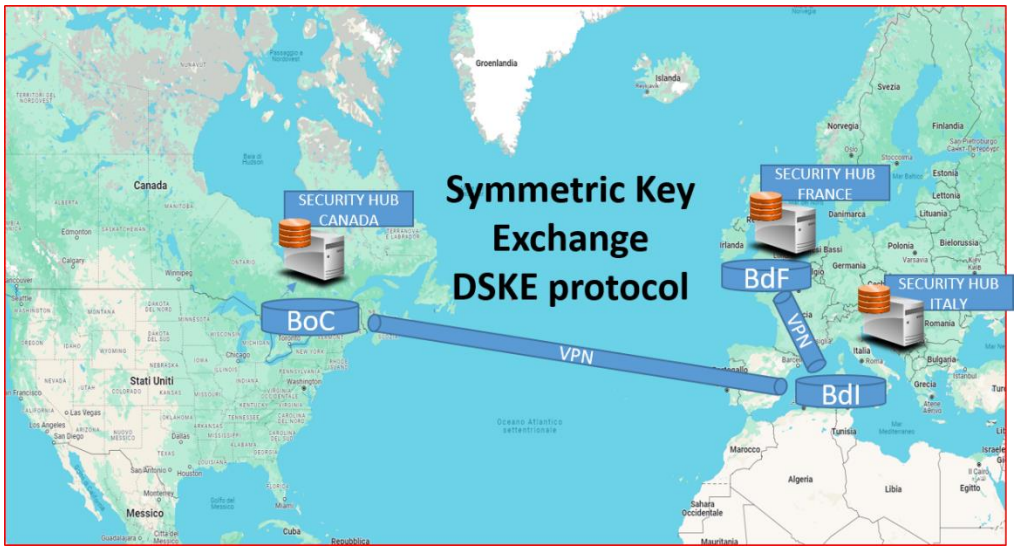


Figura 34 – Collegamento intercontinentale *quantum safe* tra tre banche centrali

All'interno della Banca d'Italia, prestatore di servizi di firma elettronica qualificata, si è ritenuto, di particolare rilievo il tema delle *Certification Authority* quantum *safe*. A tale scopo si sono svolti incontri con l'Agenzia per l'Italia digitale e l'Agenzia per la Cybersicurezza Nazionale che partecipa ai tavoli europei che seguono le certificazioni in ambito crittografico. Inoltre, si è introdotto un *Proof of Concept* basato su un software open source in grado di emettere certificati digitali basati su algoritmi post quantum anche in modalità ibrida (coesistenza di entrambi gli algoritmi all'interno dello stesso certificato). Questo ha consentito di effettuare un primo set di test funzionali e non funzionali per l'utilizzo di tali certificati. Sono previsti ulteriori test basati sul rilascio di nuovi versioni software e sulla disponibilità da parte dei *vendor* di dispositivi crittografici hardware (smart card, *Hardware Security Module* - HSM) in grado di supportare tali algoritmi.

Nell'ambito delle iniziative volte a favorire la condivisione e lo scambio di informazioni ed esperienze su tali tematiche, lo scorso febbraio si è svolto il *workshop* "Quantum Safe Communications: panoramica sullo stato dell'arte e sulle prospettive future nell'utilizzo delle tecnologie" al quale hanno partecipato rappresentanti del mondo accademico, delle istituzioni, di aziende del settore e della Banca d'Italia. Il *workshop* ha rappresentato un'occasione di confronto sull'utilizzo di tecnologie quantistiche quali QKD e PQC nell'ambito delle quantum *safe communications*.

Anche il presente studio, condotto in sede CIPA, è frutto della volontà della Banca d'Italia di aumentare le conoscenze, sensibilizzare l'intero sistema bancario e finanziario verso opportunità e rischi delle tecnologie quantistiche e porsi come riferimento per una rete di collaborazione.

6.3.2 ABI

Il consorzio ABI Lab è il Centro di Ricerca e Innovazione per la banca promosso dall'ABI (Associazione Bancaria Italiana) per facilitare il dialogo tra banche e aziende ICT. Mette in relazione banche, aziende e istituzioni per promuovere l'innovazione nel settore finanziario italiano attraverso tavoli tecnici di ricerca, progetti sperimentali e l'organizzazione di eventi e seminari sui principali temi di innovazione applicabili al mondo bancario.

In particolare, ha promosso nel 2023 una giornata di studio[124] con il coinvolgimento di protagonisti del mondo della ricerca e dell'industria dedicata all'esplorazione degli scenari emergenti sul Quantum Computing i cui atti sono disponibili ai consorziati.

A livello europeo è attivo su numerosi progetti finanziati dalla Commissione europea e gruppi di lavoro dove contribuisce alla discussione su innovazione e cybersecurity. A marzo 2024 il CERTFin - CERT Finanziario Italiano, attraverso il Consorzio, ha presentato due proposte di finanziamento per altrettanti progetti in ambito quantistico, rendendosi disponibile a coordinare tali iniziative con l'obiettivo di favorire ricadute positive per l'intera comunità bancaria.

6.3.3 Bank for International Settlements (BIS) Innovation Center

A giugno 2023 è stato lanciato il Project Leap dal BIS Innovation Hub Eurosystem Centre in collaborazione con la Banque de France e la Deutsche Bundesbank, per sensibilizzare e preparare le banche centrali e l'intero sistema finanziario alla transizione verso una crittografia quantum-resistant.

La prima fase del progetto[125] ha avuto come obiettivo la sperimentazione di una comunicazione con protocolli crittografici post-quantistici tra due banche centrali. È stato implementato un algoritmo tradizionale a chiave pubblica insieme a diversi algoritmi quantum-resistant in una modalità di cifratura ibrida, con l'obiettivo di mantenere la riservatezza dei messaggi inviati attraverso due sistemi IT distanti. Il canale di comunicazione quantum-resistant è stato utilizzato per veicolare messaggi di pagamento trasmessi tra la Banque de France e la Deutsche Bundesbank con l'obiettivo di sperimentare le prestazioni dei prodotti e dei processi esistenti utilizzando tecnologia quantum-resistant.

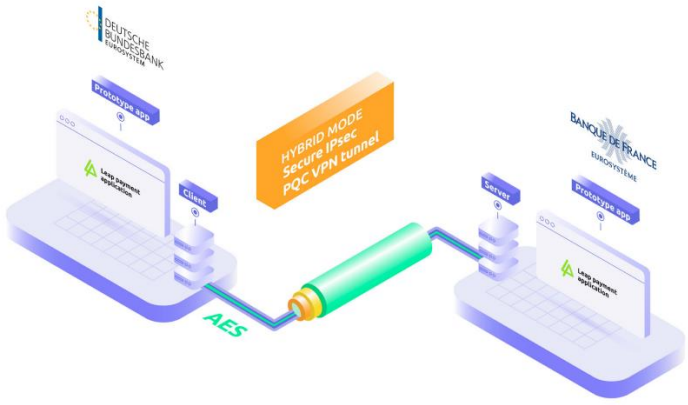


Figura 35 – VPN quantum safe realizzata con crittografia quantistica "ibrida"

Per favorire una comprensione più ampia della crittografia post-quantistica, la prima fase del progetto ha esplorato soluzioni che incorporano la nozione di *crypto agility* (introducendo la possibilità di variare l'algoritmo utilizzato per la cifra) e ha dimostrato che è possibile applicare nuovi schemi quantum-*resistant*.

Nel 2024 è partita una seconda fase del progetto, con l'obiettivo di mostrare come un sistema di pagamenti può essere protetto dalla potenziale minaccia dei computer quantistici, che potrebbero

[124] Quantum Computing - ABI Lab

[125] https://www.bis.org/publ/othp67.pdf

essere in grado di rompere i sistemi di crittografia usati attualmente per proteggere le transazioni finanziarie nei sistemi di pagamento in uso. In questa fase saranno esplorati ulteriori casi d'uso delle banche centrali con l'obiettivo generale di contribuire all'impermeabilità quantistica del sistema finanziario. Pertanto, saranno coinvolte più di due banche centrali per indagare su ambienti IT più complessi in preparazione ai contesti del mondo reale. Sarà pubblicato un nuovo rapporto che fornirà indicazioni sulle specificità dei sistemi delle banche centrali al fine di facilitare i piani di migrazione verso ambienti quantistici sicuri.

6.3.4 Bank of Canada

La Bank of Canada, in linea con le indicazioni nazionali (cfr. 8.1), è estremamente attiva nell'ambito delle sperimentazioni sul quantum *computing* e sulle strategie di prevenzione delle minacce anche tramite numerose partnership. La strategia è fondata su quattro pilastri: l'obiettivo di resiliency, la creazione di un ecosistema di collaborazione, lo sviluppo delle risorse umane e la ricerca mirata a identificare applicazioni e use cases.

Recentemente ha stretto una collaborazione con evolutionQ, una società canadese dedicata alla personalizzazione di soluzioni che utilizzano le tecnologie quantistiche, per progetti di sicurezza in particolare legate alla moneta digitale. Per questo progetto il codice sviluppato sarà reso disponibile con licenza open source con l'obiettivo di fornire strumenti alla comunità di sviluppo e accelerare il processo globale di transizione post-quantum.

Nel giugno 2023, per citare un esempio, è stato pubblicato un articolo[126] che propone l'utilizzo di tecniche post-quantum per garantire la privacy nei pagamenti e allo stesso tempo proteggere gli utenti da possibili frodi. Viene proposto un meccanismo di credenziali pratico e interattivo, in cui agli utenti vengono rilasciate credenziali pseudonime che possono essere utilizzate per registrarsi presso i fornitori di servizi finanziari senza rivelare informazioni personali. Il protocollo si è dimostrato sicuro e privo di perdite di informazioni, preservando la privacy dell'utente indipendentemente dal numero di registrazioni.

6.3.5 Intesa Sanpaolo

Intesa Sanpaolo ha istituito al suo interno, già dal 2020, un centro di competenza sulle tecnologie quantistiche[127] focalizzato a individuare le opportunità offerte dal quantum *computing* nell'ambito bancario e finanziario, occuparsi dei percorsi di crescita e di sensibilizzazione, collaborare con il mondo accademico e individuare linee guida per l'adozione di queste tecnologie.

[126] https://www.bankofcanada.ca/2023/06/staff-working-paper-2023-33/

[127] Quantum Computing in Finance: The Intesa Sanpaolo Experience | IEEE Journals & Magazine | IEEE Xplore

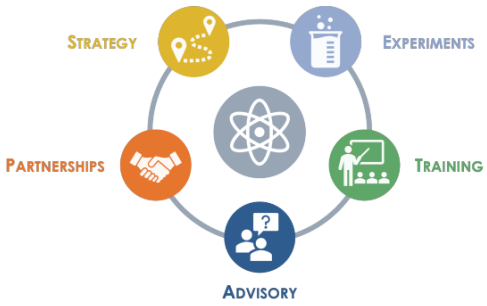


Figura 36 – Gli obiettivi del Quantum Competence Center di Banca Intesa

Sono state avviate diverse iniziative di sperimentazione che comprendono l'utilizzo di piattaforme di calcolo quantistico per test di algoritmi di *portfolio optimization*, *credit risk analyisis* e *derivative pricing*, la partecipazione a progetti di reti sicure, collaborazioni accademiche e investimenti in start up.

In particolare Intesa Sanpaolo:

- dal 2021 ha avviato, in collaborazione con gli stessi *vendor*, sperimentazioni con due differenti piattaforme di calcolo quantistico (D-Wave – attraverso Data Reply – e IBM) per approfondirne le differenti potenzialità;
- nel 2022 tramite NEVA (Venture Capital del Gruppo) ha investito nella start up Classiq, società specializzata nello sviluppo software con il focus nella creazione di una piattaforma che semplifichi il processo di disegno degli algoritmi quantistici;
- ha partecipato all'iniziativa PoliQI, una delle prime reti quantistiche metropolitane, realizzata in collaborazione con il Politecnico di Milano, la Regione Lombardia e l'Esercito Italiano che garantisce comunicazioni *quantum safe* tra il distretto finanziario, militare e istituzionale all'interno della città:

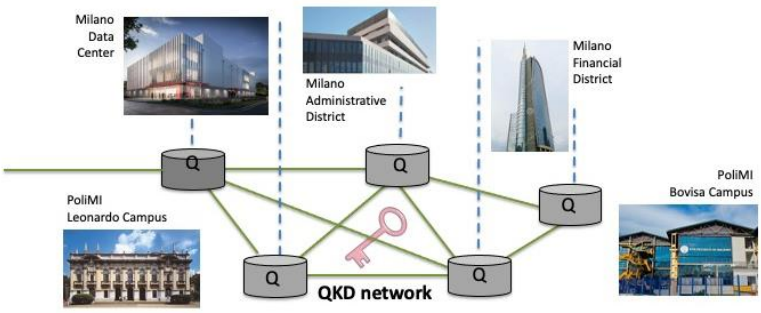


Figura 37 – Schema del POLIQI-POLItecnico Quantum Infrastructure[128]

- è partner dell'Osservatorio del Politecnico di Milano in Quantum Computing e Communication (cfr. 4.1);

[128] Fonte: Regione Lombardia e PoliMi insieme per una rete di comunicazione criptata e la ricerca sulla stampa 3D nel biomediocale - Industria Italiana

- partecipa al centro nazionale di ricerca in High Performance Computing, Big Data & Quantum Computing finanziato dai Recovery Fund EU; all'interno di questa collaborazione sono in corso di approfondimento due use cases: il primo relativo al tema della *fraud detection* (il riconoscimento di anomalie allo scopo di individuare azioni criminali perpetrate attraverso il sistema bancario) e il secondo relativo al *credit scoring* (ovvero alle modalità con cui accertare se un richiedente è in grado di sostenere un prestito). I modelli classici a questi problemi presentano delle peculiari difficoltà dovute alla particolarità della gestione dei dati in input e alla loro parametrizzazione;
- ha sostenuto la creazione nel 2022 e continua a supportare lo svolgimento delle edizioni del master in *Quantum Computing & Communication* promosso dal Politecnico di Torino sia attraverso la partecipazione di propri dipendenti, sia collaborando alla didattica;
- ha pubblicato diversi paper di ricerca industriale, tra cui un articolo peer-reviewed in collaborazione con IBM e Politecnico di Torino, nel quale si propone una variante migliorativa (nella quantità di fattori introdotti nel modello e nella flessibilità dei dati in input) di algoritmi quantistici per il *Credit Risk Assessment*, testandoli sia attraverso simulatori quantistici sia attraverso il quantum computer effettivi di IBM;
- in collaborazione con il Politecnico di Torino e la Fondazione LINKS partecipa a ricerche volte a individuare quali processi possano trarre vantaggio da un approccio quantistico e sviluppare i relativi Proof of Concept che hanno portato alla pubblicazione di diversi lavori. In particolare, le aree identificate sono: la modellazione del rischio tasso e cambio, la *default prediction*, l'*anomaly detection* e, in generale, il *quantum machine learning*;
- collabora con IBM per individuare strategie *quantum safe* e sperimentare l'impatto dell'introduzione di algoritmi *post-quantum* con progetti che permettano di verificare vari use case (da semplici comunicazioni client/server a realizzazione di VPN) utilizzando librerie del prodotto IBM Quantum Safe Remediator[129]. Inoltre ha dichiarato[130] di voler sfruttare le capacità di crittografia abilitate per l'uso di tali algoritmi offerte dal mainframe z16.

Intesa Sanpaolo diffonde pubblicamente il proprio modello organizzativo e la sua visione sull' importanza strategica di questi temi anche per promuovere l'immagine di un istituto efficiente e votato all'innovazione e punta a divenire un punto di riferimento nel panorama bancario e finanziario italiano ed europeo per questi temi.

6.3.6 BBVA

BBVA ha introdotto, a partire dal 2019, diverse linee di ricerca per investigare il valore delle tecnologie quantistiche in diversi use case. L'obiettivo, in generale, è quello di individuare e quantificare eventuali benefici, stimare le risorse computazionali necessarie per ottenerli e come queste scalino rispetto alle dimensioni del problema.

In particolare:

[129] Intesa Sanpaolo collabora con IBM nel testare soluzioni post quantistiche

[130] Intesa Sanpaolo e IBM: accordo per infrastrutture tecnologiche innovative

- ha stretto una alleanza strategica con il Consiglio Nazionale delle Ricerche Spagnolo (CSIC) per collaborare a progetti di ricerca a carattere scientifico sul disegno e il test di algoritmi quantistici utilizzabili in scenari finanziari;
- in collaborazione con Fujitsu ha sviluppato un PoC sul *quantum digital annealer* di Fujitsu (un sistema che simula l'hardware quantistico) per il problema di ottimizzazione del portafoglio (ovvero la miglior scelta di asset finanziari che, tenendo conto di vari parametri, compresa la quantificazione del rischio, fornisca il maggior guadagno per il possessore). La tipica soluzione classica a questo problema prevede di classificare gli asset a seconda dei rischi associati. Le possibili combinazioni, tuttavia, aumentano esponenzialmente in ragione degli asset e necessitano risorse di calcolo esose per l'ottimizzazione del risultato;
- ha condotto vari test con differenti fornitori per l'ottimizzazione dinamica del portafoglio, ovvero l'evoluzione delle sue performance nel tempo in relazione all'andamento del mercato. A questo scopo sono state valutate diverse piattaforme tecnologiche con la collaborazione di Accenture e della start up spagnola Multiverse. Attraverso un *proof of concept*, sviluppato insieme a quest'ultima, la banca spagnola ha messo a confronto diverse piattaforme di tecnologia quantistica per risolvere un problema classico della finanza: l'ottimizzazione dei portafogli di investimento con dati di mercato reali. Grazie a questa analisi, pubblicata anche in un articolo scientifico[131], i ricercatori hanno delineato nuove formule che potrebbero aiutare a velocizzare questo tipo di calcolo, massimizzando la redditività e minimizzando il rischio[132];
- in collaborazione con Accenture e D-Wave ha valutato margini per l'ottimizzazione del processo di *credit scoring* con la valutazione sui benefici attesi nel momento in cui vengano introdotte ulteriori variabili rispetto a quelle normalmente in uso in questi modelli;
- ha introdotto, in collaborazione con la start up Zapata Computing, un PoC per valutare l'uso degli algoritmi quantistici per ottimizzare le procedure per il calcolo del costo dei derivati, tradizionalmente effettuati tramite simulazioni Monte Carlo.

Oltre a quelli citati, BBVA ha dichiarato di volere coinvolgere anche altre unità di business per altri temi come l'ottimizzazione dei processi di Machine Learning.

6.3.7 Crédit Agricole

Nel giugno 2021, la banca francese ha avviato due progetti sperimentali con l'obiettivo di valutare il contributo di un approccio algoritmico ispirato all'informatica quantistica e il potenziale dei computer quantistici per la finanza in due rispettivi ambiti: la valutazione dei prodotti finanziari e la valutazione dei rischi di credito[133].

131 [2007.00017] Dynamic Portfolio Optimization with Real Datasets Using Quantum Processors and Quantum-Inspired Tensor Networks (arxiv.org)

132 https://www.bbva.com/en/bbva-and-multiverse-showcase-how-quantum-computing-could-help-optimize-investment-portfolio-management/

133 https://pressroom.credit-agricole.com/news/quantum-computing-two-real-world-experiments-conducted-by-credit-agricole-cib-in-partnership-with-pasqal-and-multiverse-computing-produce-conclusive-results-in-finance-cddc-94727.html

A tale scopo, la banca ha usufruito di una collaborazione con la compagnia francese Pasqal (una delle compagnie europee che progetta hardware quantistico) e la start up francese Multiverse specializzata in algoritmi quantistici.

Gli esperimenti si sono svolti nell'arco temporale di più di un anno mostrando le limitazioni note degli attuali processori ma evidenziando che il processore a 50 qubit su cui sono stati effettuati i test per la valutazione dei derivati ha mostrato la stessa accuratezza di calcolo dei sistemi tradizionali permettendo, tramite una proiezione, di stimare un miglioramento delle performance del calcolo quantistico rispetto a quello classico già con un processore a 300 qubit come già noto dalla letteratura scientifica sul tema.

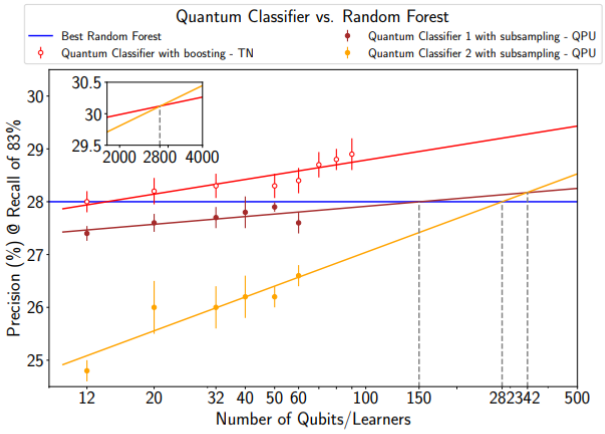


FIG. 8. Scaling of precision P of various proposed quantum classifiers with respect to the number of qubits, keeping $R = 83\%$. The two variations of the subsampling approach (yellow, brown) are implemented on QPU (filled dot) between 12 and 60 qubits. The boosting approach (red) is implemented using the TN optimizer (empty dot) between 12 and 90 qubits. The best performance of the Random Forest classifier acts as threshold (blue). The error bars represent the variability in corresponding performance across 5 iterations/QUBOs. Scaling projections are obtained by linear extrapolation (plain line).

Figura 38 – Proiezioni di confronto tra un popolare meccanismo di ML classico (Random Forest) e classificatori quantistici su tecnologia a neutral atom (Pasqal) che mostrano un break event point attorno ai 300 qubit[134]

6.3.8 Crédit Mutuel

Nel dicembre 2023, attraverso un comunicato stampa relativo al piano strategico per il triennio 2024-2027[135], il gruppo francese, uno dei più attivi nel paese, ha reso noto di aver avviato programmi di ricerca applicata in ambito quantistico, in particolare finalizzata al contrasto delle frodi e alla gestione ottimale dei rischi. L'azienda, che ha identificato un team dedicato all'interno della sua divisione tecnologica Euro-Information, ha intrapreso una collaborazione da diversi anni con IBM che ha previsto una prima fase di apprendimento di conoscenze sul funzionamento del quantum computing e sull'utilizzo del SDK di IBM. L'obiettivo più recente è introdurre una Quantum Factory, una struttura collaborativa composta da esperti tecnologici e di settore che contribuiscano a diffondere consapevolezza sui temi quantum e preparino il processo di integrazione di queste tecnologie.

[134] 2212.03223.pdf (arxiv.org)

[135] https://investors.bfcm.creditmutuel.fr/static-files/2dea8d23-96b3-4eff-924a-d91a3dafddfe

6.3.9 JP Morgan

Il reparto R&D di JPMorgan è da anni estremamente attivo nel condurre ricerche su tecnologie di frontiera e non fa eccezione l'ambito quantistico, con due filoni separati focalizzati rispettivamente sul quantum *computing* e sulle quantum *communication*. L'organizzazione societaria ha previsto l'identificazione di un team dedicato a questi temi.

Gli *use case* oggetto di approfondimento sono numerosi e possono essere visionati direttamente sul sito dedicato[136]; si riporta qui una breve sintesi.

Per quanto riguarda le opportunità offerte del calcolo quantistico, JP Morgan si è dedicata, al momento, ad un vasto ventaglio di use case (ottimizzazione del portafoglio, stima dei derivati, analisi del rischio, applicazioni nel campo del Machine Learning in vari scenari, dall'individuazione delle frodi al Natural Language Processing).

Inoltre, in collaborazione con Toshiba e Ciena, ha realizzato un prototipo sulla trasmissione sicura tramite QKD in area metropolitana (in particolare una trasmissione a 800 Gbps in condizioni ambientali standard[137]).

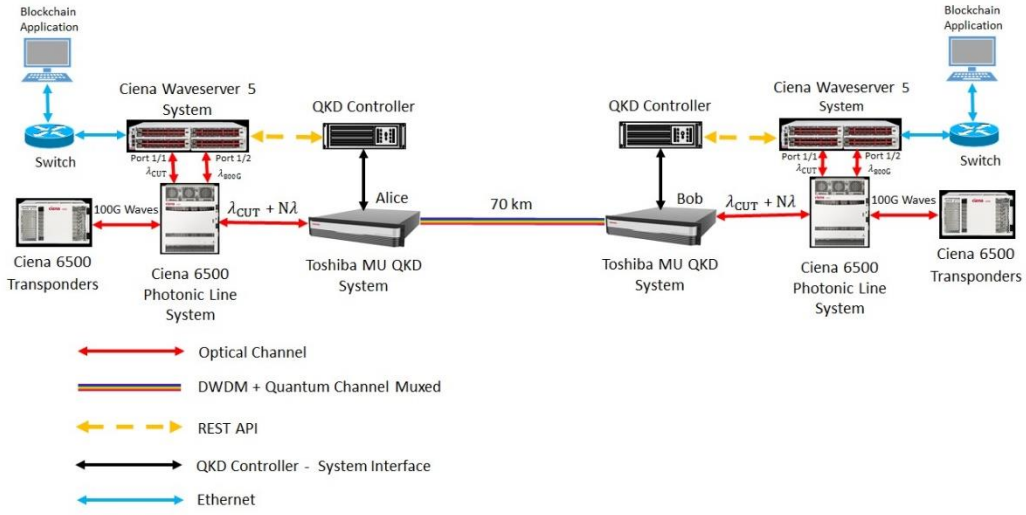


Figura 39 - Setup realizzato da JPMorgan in collaborazione con Toshiba e Ciena per il test di trasmissione quantum safe di dati di un'applicazione blockchain.

JPMorgan, come altri enti finanziari, ha scelto di investitire (300 milioni di dollari) in una start up di calcolo quantistico (Quantinuum) con cui ha una collaborazione dal 2020. Il nuovo capitale viene destinato all'avanzamento dei suoi sistemi di calcolo quantistico (basati su *trapped ions*) e all'ampliamento delle funzionalità del software quantistico che mette a disposizione.

136 https://www.jpmorgan.com/technology/applied-research

137 https://www.jpmorganchase.com/content/dam/jpm/cib/complex/content/technology/publications/qkd-research-prototype-project-5-1.pdf

6.3.10 HSBC

L'istituto ha creato al suo interno un team di ricerca quantistica finalizzato allo sviluppo di *use case* e relativi brevetti. Il team collabora con una serie di player internazionali come IBM, Fujitsu e Quantinuum, ma anche con il mondo accademico e istituzioni governative[138].

Anche HSBC, con la collaborazione di British Telecom, utilizzando i devices di Toshiba ha testato una piattaforma di trading cifrando i dati tramite QKD.

6.3.11 Gruppo Santander

Il gruppo Santander ha introdotto dal 2019 un gruppo focalizzato sulla sicurezza (Quantum Threat Group) che nel 2022 ha definito il "Quantum Threat Program", un programma a lungo termine per la transazione ad una crittografia quantum safe.

In collaborazione con Microsoft, ha reso disponibile su gitlab un tool open source[139] per l'identificazione di vulnerabilità e uno[140] per l'interpretazione dei risultati.

Il gruppo è molto attivo nella partecipazione in comitati internazionali e nella divulgazione di pratiche legate alla sicurezza quantistica. In particolare:

- partecipa attivamente al consorzio, con HSBC e JPMorgan, del centro di eccellenza della National Cybersecurity US al progetto di Migrazione Post-Quantum;
- è coinvolto nelle attività del World Economic Forum e nella componente spagnola del progetto EuroQCI (cfr. 4.3.2.3);
- è parte del consorzio spagnolo Caramuel[141] per valutare comunicazioni quantistiche via satellite;
- è parte dello steering commitee del Quantum Safe Financial Forum[142], creato dall'Europol European Cybercrime Center focalizzato sulla transazione post quantum.

L'analisi di confronto tra varie strategie quantum safe proposta nel capitolo 5 del presente resoconto è tratta da una presentazione[143] mostrata da Santander durante la conferenza PQC tenutasi ad Amsterdam nel 2023.

Santander è impegnato anche sul fronte del quantum *computing*, con la pubblicazione di diversi articoli scientifici.

138 https://www.hsbc.com/who-we-are/businesses-and-customers/hsbc-and-quantum

139 https://codeql.github.com/

140 https://github.com/Santandersecurityresearch/cryptobom-forge

141 https://www.hispasat.com/en/press-room/press-releases/archivo-2022/449/un-grupo-de-empresas-espanolas-lideradas-por-hispasat-trabaja-en-la-fase-de-viabilidad-de-caramuel-la-primera-mision-geoestacionaria-de-distribucion-cuantica-de-claves

142 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff

143 https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jaime-gomez_banco-santander_comparing-strategies-for-quantum-safe-cryptography-adoption-in-organizations.pdf

6.3.12 I dati della rilevazione della Convenzione Interbancaria Per l'Automazione (CIPA)

Nel rapporto sulla "Rilevazione sull'IT nel settore bancario italiano - Profili economici e organizzativi"[144], relativa al 2022, sono riportati i risultati dell'analisi dedicata al tema delle tecnologie quantistiche nel settore bancario realizzata dalla CIPA. La Rilevazione ha affrontato sia il profilo delle opportunità che dei rischi di tali tecnologie, fotografando la situazione al 2022 nonché la previsione per il biennio 2023-2024. Dall'indagine, a cui hanno partecipato 21 gruppi bancari, che rappresentano il 92,5% dell'insieme dei gruppi in termini di totale attivo, e 33 banche, è emerso che sette gruppi hanno avviato attività di analisi/studio o sperimentazione sul quantum e un gruppo prevede di farlo entro il 2024, mentre oltre la metà del campione non ha avviato e non prevede di avviare iniziative sul quantum entro il 2024.

L'ambito di studio/ricerca più rilevante risulta quello degli algoritmi quantistici finalizzati al miglioramento delle prestazioni (quattro su sette gruppi rispondenti). Sul fronte della post-quantum *cryptography* sono attivi due gruppi, numero che cresce in previsione entro il 2024 soprattutto nelle attività di analisi del proprio parco applicativo e adozione di algoritmi di crittografia quantum *safe* su sistemi tradizionali.

Dalla Rilevazione emerge inoltre che le competenze nell'ambito delle tecnologie quantistiche vengono reperite soprattutto mediante collaborazioni con il mondo accademico e della ricerca, a cui si affiancano anche altre modalità quali le consulenze e la formazione specifica.

[144] https://www.cipa.it/rilevazioni/economiche/2022/Rilevazione_economica_2022.pdf

7 Conclusioni

Il gruppo di lavoro ritiene di condividere, riassumendole nel seguito, le principali considerazioni emerse nel corso delle attività di analisi e ricerca sui vari temi affrontati nel documento e nel confronto delle differenti esperienze. Appare evidente che ogni indicazione sia da valutarsi all'interno di ogni singola organizzazione, tenendo conto delle sue specificità in termini di necessità di business, prospettive di innovazione, disponibilità di investimento e opportunità strategiche.

Anzitutto, è emerso un generale apprezzamento verso l'attenzione di istituzioni, come Banca d'Italia e ABI, nello stimolare l'approfondimento di questa materia, a fronte di investimenti e iniziative nazionali circoscritte, sia nel settore pubblico sia in quello privato, rispetto al panorama europeo e internazionale. Si ritiene, infatti, a questo stadio di disponibilità della tecnologia, che il tema della consapevolezza sia uno dei più sfidanti, soprattutto allo scopo di ottenere il supporto esecutivo della più alta linea manageriale.

La stessa possibilità di confronto tra differenti operatori è ritenuta fondamentale e dovrebbe essere incoraggiata a tutti i livelli aziendali. In questa fase precompetitiva, si ritiene non ci sia alcun fattore ostativo nel condividere le esperienze portate avanti dalle singole imprese, bensì si possa determinare un beneficio complessivo nel mettere a fattor comune le diverse esperienze. Questo modello è pubblicamente perseguito con successo da società internazionali come JP Morgan, HSBC e Santander.

La partecipazione a eventi nazionali e internazionali (cfr. 4.1) è considerata una valida opportunità per creare una rete di conoscenze, identificare interlocutori e valutare differenti casi d'uso. L'attenzione alle iniziative istituzionali, allo stato di definizione degli standard e all'aggiornamento sugli avanzamenti in campo della ricerca accademica e industriale, è ritenuta essenziale per agevolare un proficuo approccio a questi temi.

Si ritiene che la principale sfida nel contesto aziendale sia la capacità di veicolare l'importanza di intraprendere da subito investimenti dedicati, spesso limitata dalla difficoltà di percepire un valore adeguato di ritorno di investimento (ROI) in un orizzonte temporale di breve e medio termine a fronte di un'offerta di mercato non sempre matura e convincente.

Le tecnologie quantistiche per loro natura si prospettano, una volta a regime, come tecnologie di grande impatto, ma con ridotta disponibilità sul mercato. I rischi di investimenti tardivi potrebbero quindi concretizzarsi nel momento in cui, una volta che la tecnologia sia matura, il mercato non offra un accesso diffuso a questi strumenti, portando uno svantaggio competitivo agli attori che non abbiano investito per tempo[145].

Inoltre, la necessità di affrontare i rischi di compromissione della sicurezza di dati e transazioni, connessi con la disponibilità di elaborazione quantistica, deve prevedere il coinvolgimento di tutti

[145] Nel suo documento indirizzato al sistema finanziario inglese (Minimising the risk: quantum technology and financial services - https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial) UK finance identifica come aree di rischio in relazione all'avvento di queste tecnologie non solo la possibilità che la crittografia tradizionale venga compromessa ma pure una possibile instabilità di mercato generata dal mancato investimento in queste opportunità. Questo scenario risulta aggravato dalla penuria di competenze ed esperienza nel campo e dal debito tecnologico dei sistemi legacy.

gli attori, in modo particolare nel contesto bancario e finanziario dove una vulnerabilità emersa e resa pubblica potrebbe mettere a rischio l'affidabilità e la reputazione dell'intero sistema.

È essenziale veicolare il messaggio che, nonostante ci sia difformità di vedute sugli orizzonti temporali di disponibilità del calcolo quantistico, il tempo necessario affinché diventino vulnerabili gli attuali algoritmi asimmetrici di cifratura potrebbe essere più contenuto di quanto prospettato, anche solo grazie ai progressi nella criptoanalisi classica. Inoltre, le attività richieste per l'adeguamento delle soluzioni IT sono onerose e richiedono una adeguata pianificazione. Alcune delle procedure propedeutiche all'introduzione di tali presidi risultano proficue in modo indipendente dal rischio "quantum", in quanto identificare sistemi e processi che dipendono da crittografia potenzialmente vulnerabile e prioritizzare le risorse da proteggere (dati personali, transazioni, contratti, ecc.) rappresentano tradizionali processi di *continuous improvement*[146]. Inoltre focalizzarsi sulla *crypto agility* e individuare soluzioni flessibili, che si possano aggiornare o modificare con facilità, può rappresentare un'occasione per rinnovare il *framework* applicativo che, in alcuni casi, può risultare frammentato e stratificato da diverse evoluzioni e manutenzioni.

Nonostante l'ambito della sicurezza rappresenti una priorità per le banche, si ritiene opportuno anche invitare a sviluppare una strategia per l'adozione del quantum *computing* nei settori di business, come per la soluzione di problemi di ottimizzazione e simulazione stocastica nell'ambito dei processi finanziari[147].

Per rendere il più vantaggioso possibile questo approccio, è necessario partire da un inventario di quelle applicazioni di business che potrebbero trarre giovamento da questo nuovo paradigma di calcolo, in termini sia di velocità di calcolo, sia di accuratezza dei risultati e, non ultimo, numero di risorse computazionali richieste a garantire tali tempestività e precisione nella generazione degli output.

Ancorché sia emerso qualche scetticismo, giustificato più che altro dal fatto che, almeno per alcuni, esistano già alternative percorribili nel breve termine con l'utilizzo di altri strumenti di *accelerated computing* (GPU, TPU[148], ecc.), la superiorità teorica di alcuni algoritmi quantistici in prospettiva resta un dato di fatto, scientificamente provato. A tale proposito, non può trascurarsi la riflessione sull'impatto ambientale dovuto all'utilizzo energivoro degli strumenti classici a fronte di consumi nettamente più contenuti a parità di tempo di calcolo, ad esempio per il raffreddamento dei computer quantistici a superconduttori[149].

[146] A questo proposito si segnala che alcune indicazioni contenute nel recente regolamento DORA (Digital Operational Resilience Act, Cpt.1 Art.6 e 7) e negli standard di sicurezza per i pagamenti elettronici PCI DSS 4.0 (12.3.3) fanno riferimento alla realizzazione di inventory (*crypto asset*) e di processi (*crypto agility*). Tali iniziative saranno quindi incluse nelle attività di compliance richieste in questo ambito da realizzare entro il 2025.

[147] . È ragionevole ipotizzare che il prossimo futuro vedrà forti sviluppi su questi temi, con la realizzazione di applicazioni industriali basate su quantum *machine learning* e altre tecnologie quantistiche.

[148] Graphical Processing Unit (GPU) e Tensor Processing Unit (TPU) sono processori specializzati realizzati per accelerare alcune funzioni elaborative specifiche rispetto alle CPU tradizionali.

[149] Va segnalato a questo proposito che altre tecnologie di *qubit* allo studio nemmeno richiedono l'ausilio di tecnologia criogenica per il loro funzionamento.

Per quanto concerne gli aspetti economici, l'esperienza dei partecipanti al gruppo indica che la spesa per l'introduzione di PoC per sperimentare un *crypto assessment* o l'utilizzo di software post-quantum *safe* nonché l'accesso a risorse di elaborazione quantistica in cloud (o loro simulazione) per valutare gli *use case* di maggior interesse potrebbe risultare contenuta[150].

A questo proposito, si ritiene utile anche suggerire la possibilità di accedere a risorse comunitarie partecipando a progetti finanziati dalla Commissione europea (ad esempio paragrafo 4.3.2.2).

Il CERTFin, che a marzo 2024, attraverso il Consorzio ABI Lab, ha già sottomesso due proposte di finanziamento per altrettanti progetti in ambito quantistico, si rende disponibile a coordinare tali iniziative con l'obiettivo di favorire ricadute positive per l'intera comunità bancaria.

Un ultimo aspetto di particolare rilievo è relativo alle competenze necessarie. Si è riscontrata una generale difficoltà a reperire risorse umane con preparazione adeguata, vista la grande specificità delle competenze richieste e la trasversalità delle stesse in differenti ambiti, come l'informatica, la fisica e la conoscenza di dominio del settore di applicazione specifico di indagine. Risulta significativa, a questo proposito, la proposta di individuare partnership con il mondo accademico e con centri di ricerca per attrarre talenti e favorire la loro crescita. In tale ambito esistono molteplici realtà nel nostro Paese, parte delle quali è stata descritta anche in questo resoconto.

Considerando le riflessioni sopra esposte, si incoraggiano gli istituti bancari e finanziari a riflettere sull'importanza di definire una posizione chiara nell'ambito delle tecnologie quantistiche. A seconda del contesto, potrebbe risultare vantaggioso elaborare una strategia specifica oppure semplicemente riconsiderare il processo di gestione del rischio.

Nel descrivere le opportunità e le dinamiche di questo complesso ecosistema emergente, l'auspicio dei partecipanti al gruppo di lavoro è che si instauri una rete di collaborazione proficua tra aziende, istituzioni, industria e ricerca promuovendo in questo modo una crescita collettiva.

[150] Riguardo alle specifiche scelte tecnologiche o di partner commerciali con cui avviare eventuali percorsi di collaborazione, sono stati analizzati pro e contro dei due differenti approcci che vedono, da una parte, l'esclusività nella scelta del fornitore unico e dall'altra una pluralità di accordi nei confronti di venditori specifici. Nel primo caso, oltre al vantaggio di dover gestire un unico *stack* tecnologico end-to-end, l'offerta si accompagna spesso a percorsi di training e assistenza completi. Nel secondo caso, sperimentare soluzioni hardware e software differenti, pur comportando una maggiore complessità di gestione, riduce il rischio di *lock-in* e rende più agevole un cambio di rotta nel momento in cui un paradigma tecnologico dovesse risultare non competitivo nel lungo termine. In ogni caso, pare sensato iniziare ad avviare *roadmap*, PoC e prototipi, partendo dai vendor con cui già si hanno rapporti commerciali consolidati. Un'ipotesi da valutare è anche quella di investire in start up impegnate nella ricerca in ambito quantistico, contribuendo contemporaneamente al proprio e al loro sviluppo.

8 Approfondimenti

8.1 *National* quantum *strategies*

L'Australia ha investito fin dal 2015 in tecnologie quantistiche nell'ambito della National Innovation and Science Agenda e poi con l'Australian Next Generation Technologies Fund e istituito vari centri di eccellenza quantum, tra cui il Center for Quantum Computation and Communication Technology. Nel giugno 2023 ha lanciato la strategia nazionale sulle tecnologie quantistiche per il periodo 2023-2030, basata su cinque temi principali: ricerca e sviluppo, investimenti in tecnologie quantistiche *industry-ready*; accesso alle infrastrutture e ai materiali quantistici essenziali; forza lavoro qualificata; standard e *framework*; costruire un ecosistema quantistico nazionale. Oltre al piano nazionale l'Australia ha anche stabilito partnership con gli USA, con l'Università di Singapore (per la creazione di satelliti per le telecomunicazioni quantum) e con il Giappone.

Il Canada ha definito la propria strategia nazionale nel gennaio 2023 stabilendo l'allocazione dei fondi (CAN $360 milioni) stanziati nell'aprile 2021 in ricerca, istruzione e sviluppo di talenti, e commercializzazione. Nel 2023 è stato inoltre definito il piano di investimenti per l'implementazione della strategia nel campo della difesa basata su tecnologia quantistica, il programma Quantum 2030. Oltre al piano nazionale il Canada ha anche stabilito diverse partnership tra cui nel 2022 quella con l'Unione europea nell'ambito dell'EU Quantum Flagship, con tre progetti di ricerca (MIRAQLS per il *sensing*, FoQaCiA per gli algoritmi quantistici, HYPERSPACE per le comunicazioni) e con la Francia nell'ambito del Canada-France Quantum Alliance.

La Germania ha investito fin dal 2018 in tecnologie quantistiche, e nel 2023 ha annunciato altri investimenti per lo sviluppo di un computer quantistico di grandi dimensioni (tra i 100 e 500 *qubit*) entro il 2026.

La Francia ha formalmente lanciato la propria strategia per il periodo 2021-2025 nel 2021. Oltre a progetti di ricerca, infrastrutture, formazione, sicurezza, parte di questa strategia è l'installazione di una piattaforma ibrida HPC/quantum nel centro Très Grand Centre de Calcul - TGCC gestito dal Commissariat à l'énergie atomique et aux énergies alternatives – CEA comprendente il supercomputer Joliot-Curie, due quantum computer Pasqal a 100 *qubit*, un *photonic* quantum computer e un ambiente di emulazione quantum completo.

Nel 2019 i Paesi Bassi hanno pubblicato la National Agenda on Quantum Technologies e nel 2021 e nel 2022 hanno stanziato fondi per i prossimi sette anni. Nella strategia sono evidenziate quattro linee di azione (ricerca e innovazione; sviluppo dell'ecosistema, creazione del mercato e delle infrastrutture; capitale umano: istruzione, conoscenze e competenze; dialogo sociale sulla tecnologia quantistica) e tre programmi di sviluppo (quantum *computing* e simulazioni, rete quantum nazionale, applicazioni quantum *sensing*). Nel 2021 e nel 2022 sono stati stanziati i fondi dedicati alla National Agenda fino al 2027. Nel 2015 erano già stati stanziati dei fondi per un periodo di dieci anni per lo sviluppo del primo quantum computer.

La Danimarca ha lanciato la strategia nazionale per il periodo 2023-2027 in due parti, rispettivamente a giugno e a settembre 2023. La prima è incentrata sulla ricerca internazionale, sull'innovazione, sugli investimenti strategici e di lungo periodo, sul miglioramento dell'accesso alle

infrastrutture di ricerca con l'obiettivo di convertire la ricerca in nuove tecnologie applicabili. La seconda parte è dedicata al supporto allo sviluppo, commercializzazione e applicazione delle tecnologie quantistiche a beneficio della società, dell'economia, della sicurezza e della cooperazione internazionale. La Danimarca ospita anche il Centro NATO per le tecnologie quantistiche, parte del programma Defense Innovation Accelerator for the North Atlantic - Diana che ha l'obiettivo di promuovere nuove tecnologie nei paesi dell'Alleanza e comprende un incubatore di progetti, un centro di test e un laboratorio. L'iniziativa è parte del progetto NATO-2030 che prevede la realizzazione di centri di test e/o programmi di promozione delle diverse tecnologie innovative nelle nazioni della NATO.

L'Irlanda ha istituito nel 2020 un Quantum Center of Excellence. Nel novembre 2023 ha lanciato la strategia nazionale denominata Quantum 2030 organizzata su cinque pilastri (ricerca – formazione - collaborazione nazionale e internazionale - innovazione, capacità imprenditoriale e competitività economica - consapevolezza dei benefici delle tecnologie quantistiche).

L'Austria ha definito un piano di investimenti nel giugno 2021 per il periodo 2022-2026.

Il Regno Unito ha definito il proprio piano (National Quantum Technologies Programme – NQTP) nel novembre 2013. Nel 2019 è stata lanciata la fase due con investimenti per il periodo 2019-2024, mentre nel marzo 2023 il governo ha annunciato la fase 3 con nuovi fondi per il periodo 2024-2033. Le attività sono coordinate dall'Engineering and Physical Sciences Research Council. Inizialmente i fondi sono stati destinati principalmente a quattro *hub* specializzati nel *computing*, sicurezza, comunicazioni e sensori. A questi si è aggiunto nella seconda fase il National Quantum Computing Centre – NQCC con il compito di sviluppare NISQ e LSQ computers, algoritmi, software quantistici.

Oltre ai piani nazionali numerose sono le collaborazioni tra le nazioni, come quella tra Francia, Germania, e Paesi Bassi firmata nel 2022 per incrementare le sinergie con lo sviluppo di progetti condivisi, quelle bilaterali tra gli USA e diversi paesi europei come Francia, Finlandia, Svezia, Danimarca, Svizzera e UK. A inizio dicembre 2023, 11 Stati membri (Francia, Belgio, Croazia, Grecia, Finlandia, Slovacchia, Slovenia, Repubblica Ceca, Malta, Estonia e Spagna) hanno approvato una dichiarazione europea sull'importanza strategica delle tecnologie quantistiche per la competitività scientifica e industriale dell'Unione europea, impegnandosi a collaborare allo sviluppo di un ecosistema tecnologico quantistico.

8.2 Fasi per una quantum *safe transition*

8.2.1 *Awareness*

Per sensibilizzare alla necessità di pianificare un processo di migrazione verso tecnologie quantum *safe*, è fondamentale adottare un approccio strategico e coinvolgente. A tale scopo, può essere utile organizzare workshop e sessioni informative che illustrino in modo chiaro le implicazioni della computazione quantistica per la sicurezza informatica.

In parallelo, è necessario condurre analisi approfondite sulla propria infrastruttura tecnologica, valutando la maturità e la robustezza dei sistemi di sicurezza informatica esistenti. Queste valutazioni dovrebbero evidenziare potenziali vulnerabilità e punti critici che potrebbero essere esposti dall'avvento della computazione quantistica.

8.2.2 *Define*

Per descrivere la fase del processo di migrazione verso tecnologie quantum *safe* nel contesto bancario, è fondamentale definire chiaramente gli obiettivi strategici dell'iniziativa. Probabilmente, limitare il perimetro alla sicurezza dei soli sistemi di pagamento potrebbe non essere sufficiente.

Gli obiettivi strategici devono mirare a raggiungere una maggiore maturità di tutto l'ecosistema e non solo della catena dei pagamenti, assicurando ad esempio una migliore protezione delle infrastrutture e dei dati sensibili da esse gestiti, garantendo al contempo la continuità operativa e il rispetto delle normative di sicurezza e privacy.

Una volta stabiliti gli obiettivi, è necessario sviluppare una strategia dettagliata che delinei le azioni e le risorse necessarie per raggiungerli. In questo senso, è opportuno che vengano adottati approcci sistematici per la migrazione da algoritmi vulnerabili ad algoritmi quantum *resistant* nel rispetto della compatibilità con la tecnologia di supporto sottostante.

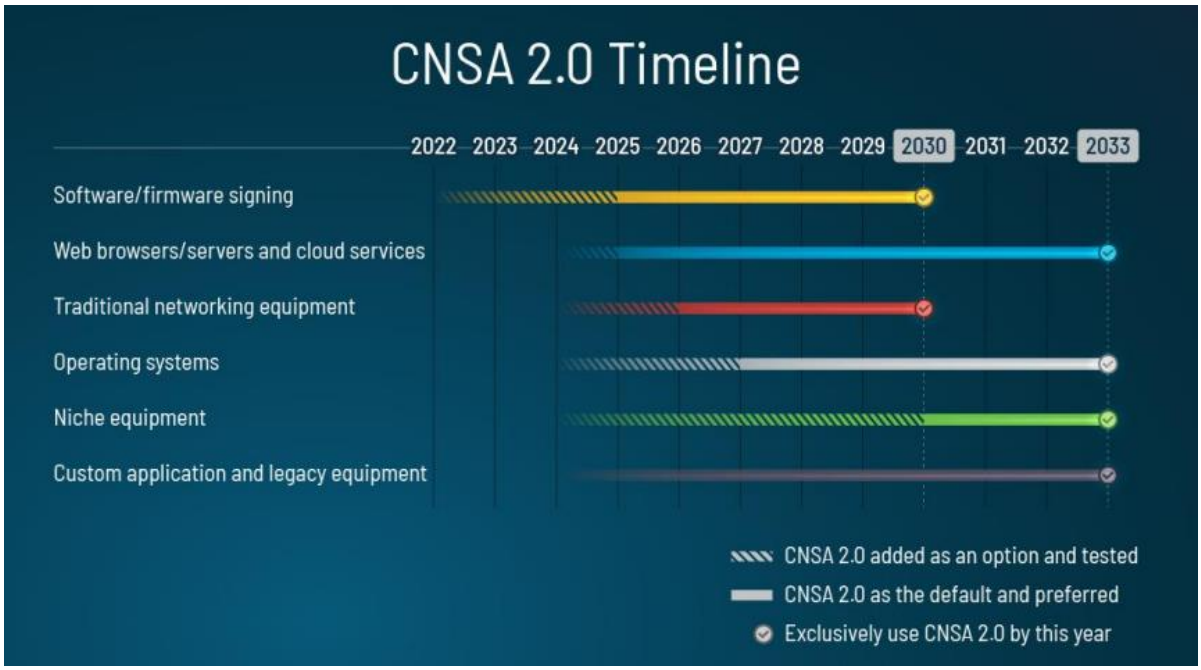
Le azioni da porre in atto sono:

- redigere un inventario per determinare quali sistemi utilizzino la crittografia a chiave pubblica e in che modo essi siano impiegati per proteggere la riservatezza e/o l'integrità delle informazioni utilizzate, scambiate o archiviate;
- supportare l'industria nell'identificazione di standard e prodotti emergenti in ambito quantistico, accrescendo la consapevolezza in merito alle caratteristiche tecniche delle soluzioni che andranno a sostituire i componenti potenzialmente vulnerabili;
- identificare tempestivamente i vincoli tecnici, al fine di risolvere eventuali incompatibilità;
- collaborare con fornitori di servizi, partner e altri stakeholder per coordinare al meglio l'adozione delle soluzioni tecniche necessarie a mantenere l'interoperabilità e la continuità operativa dei sistemi crittografici.

La costruzione di una *roadmap* è cruciale per pianificare e coordinare le attività di migrazione nel tempo. Questa *roadmap* dovrebbe stabilire una sequenza logica di passaggi, indicando chiaramente gli attori coinvolti, le fasi di implementazione delle soluzioni, i tempi previsti per ciascuna fase e le dipendenze tra le attività.

Qui di seguito un'immagine con un esempio di piano di migrazione definito dalla National Security Agency (NSA) relativamente al Commercial National Security Algorithm Suite (CNSA)[151].

[151] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF



La stima del budget necessario è un'altra componente critica di questa fase e dell'intero processo. È importante valutare accuratamente i costi associati all'acquisizione di tecnologie quantum *safe*, all'aggiornamento dell'infrastruttura e dei sistemi esistenti, alla formazione del personale e alla gestione del cambiamento. Questa stima dovrebbe tenere conto di eventuali rischi e imprevisti durante l'implementazione.

Infine, la creazione di un gruppo di lavoro dedicato è essenziale per guidare e coordinare l'intero processo di migrazione. Questo gruppo dovrebbe comporsi di esperti di sicurezza informatica e specialisti tecnici delle varie funzioni aziendali coinvolte, ma, soprattutto, dovrebbe poter contare sulla *sponsorship* del top management. La collaborazione e il coinvolgimento di diverse competenze e prospettive sono infatti fondamentali per il successo dell'iniziativa.

Le aspettative nel breve termine dovranno necessariamente includere il completamento dell'analisi dei requisiti, la selezione delle soluzioni quantum *safe* e la definizione della strategia di implementazione. Nel medio termine, ci si attende di completare la migrazione dei sistemi critici e di integrare le nuove tecnologie nell'ambiente operativo. Nel lungo termine, l'obiettivo è garantire una protezione duratura e resiliente contro le minacce emergenti, mantenendo al contempo l'efficienza e l'agilità operativa del settore bancario.

8.2.3 *Identify*

In questa fase dovranno essere identificati tutti gli ambiti dove sono utilizzati algoritmi di cifratura (applicazioni, hardware e servizi) e la tipologia stessa di tali algoritmi, sia internamente all'azienda sia dalle terze parti ritenute critiche. Lo scopo primario è quello di costruire un *crypto inventory*, facilmente consultabile e costantemente aggiornato, tale da permettere la facile individuazione di eventuali criticità e consentire una prima valutazione sugli impatti derivanti da una potenziale sostituzione delle metodologie di cifratura utilizzate.

8.2.3.1 *Crypto Discovery*

Al fine di popolare un *crypto inventory* è necessario un passaggio propedeutico: utilizzare tool di *crypto discovery*. A oggi non esiste un unico strumento in grado di interfacciarsi con tutti i verticali *legacy* e/o *open* presenti nel mercato (ad esempio mainframe, AS400, Oracle DB, MS-SQL, NAS/SAN, ecc.) ed è molto probabile che un simile strumento non sia mai disponibile a causa della forte eterogeneità che caratterizza le tecnologie adottate per realizzarli.

Gli artefatti crittografici posso essere recuperati con *network scanner* (per intercettare protocolli come SSH, TLS, IPSec, ecc.), scansione di *filesystem* per individuare certificati, chiavi di cifratura, ecc., o con altri strumenti in grado di analizzare, staticamente o dinamicamente, il codice sorgente. In generale, i software che rientrano nella categoria SAST (*Static Application Security Testing*) sono potenzialmente in grado di recuperare artefatti crittografici direttamente dal codice sorgente. Tuttavia, solo una scansione dinamica (tracciamento *run-time*) permette di individuare gli algoritmi realmente utilizzati e intercettare il caricamento effettivo di librerie esterne.

Esistono diversi software open source che possono scansionare server SSL/TLS al fine di recuperare informazioni dettagliate sugli algoritmi di cifratura utilizzati come, ad esempio, SSLScan, TLS_prober, TestSSL.sh o NMAP stesso. Parallelamente, esistono anche software proprietari che permettono di scansionare solo specifiche tecnologie (quali mainframe o apparati di rete).

8.2.3.2 *Crypto Inventory*

Un inventario crittografico è un utile strumento che raccoglie informazioni relative alle soluzioni in uso, ne classifica l'importanza e la relazione con i processi di business e identifica le variabili crittografiche utilizzate. Tale inventario si rende utile indipendentemente dalla minaccia quantistica dato che permette di evidenziare anche l'eventuale utilizzo di algoritmi obsoleti (es. Data Encryption Standard - DES) che renderebbe le applicazioni già esposte a rischi di sicurezza.

In accordo a quanto suggerito dal NIST, un inventario dovrebbe contenere almeno le seguenti informazioni di base:

- Algoritmi di cifratura utilizzati:
    - Applicazione
    - Tipologia (es.: AES, RSA, ECC), versione e lunghezza della chiave (es. 256 bit)
    - Modalità di funzionamento (ad esempio: AES ECB, CBC, CTR)
    - Finalità dell'utilizzo (integrità, confidenzialità, ecc.)
- Protocolli utilizzati:
    - Applicazione
    - Tipologia (es.: SSH, TLS) e versione
- Libreria di cifratura utilizzate:
    - Applicazione
    - Nome Libreria
    - Vendor

    - Tipologia di licenza (software proprietario, open source, …)
- Certificati digitali:
    - Applicazione
    - Ubicazione del certificato
    - Tipologia (RSA, ECC) e versione
    - Date di creazione e scadenza

Una volta censite queste informazioni, è necessario determinare anche le caratteristiche di utilizzo:

- dimensioni attuali delle chiavi e limiti hardware/software sulle dimensioni future delle chiavi e delle firme;
- soglie di latenza e throughput;
- processi e protocolli di *handshake* per la creazione delle chiavi;
- posizione di ogni processo crittografico nello *stack*;
- modalità di invocazione del processo crittografico (ad esempio, tramite chiamata a libreria crittografica, piuttosto che utilizzando un processo incorporato nel sistema operativo, utilizzando la crittografia come servizio, ecc.);
- *owner*/provider di ciascun hardware/software/processo crittografico;
- livello di agilità nell'integrazione dell'hardware/software/processo crittografico;
- condizioni contrattuali e legali imposte da e sul fornitore;
- durata del supporto e data prevista di *end-of-life* del prodotto, se dichiarata dal fornitore.

Il *crypto inventory* dovrebbe racchiudere sia le informazioni relative agli ambienti *on-premise*, sia le informazioni che si riferiscono ad ambienti *off-premise* come, ad esempio, *private*/*hybrid*/*public* cloud. Inoltre, una volta completata la sua redazione, si dovrà periodicamente verificare la coerenza tra il contenuto dell'inventario e quanto previsto dalle policy di sicurezza interne.

Anche le componenti hardware (HSM, PKI, *appliance* VPN, firewall, IDS, ecc.) contengono artefatti crittografici e la capacità di utilizzare algoritmi specifici. Data la rilevanza e il ruolo che essi giocano nella sicurezza aziendale, l'inclusione di tali apparati nel *crypto inventory* è essenziale.

Le informazioni provenienti da terze parti (outsourcing, applicazioni SaaS, ecc.) dovrebbero essere inserite anch'esse all'interno del database. Tuttavia, va tenuto conto che le autodichiarazioni dei fornitori (o dei *vendor*) potrebbero portare all'inserimento di informazioni parziali e/o errate con il rischio di generare falsi positivi o falsi negativi.

Infine, per agevolare la pianificazione di una migrazione efficace, può essere molto utile integrare nell'inventario anche informazioni relative a casi d'uso concreti. In questo ci viene in aiuto il già

citato documento “Canadian National Quantum – Readiness”[152] dove, negli Annex D, E ed F, sono descritti alcuni esempi come l’autenticazione Kerberos, i sistemi PKI/CAs e il protocollo sFTP.

Tali scenari vengono analizzati e inventariati secondo questo schema:

- Descrizione del caso d'uso
- Valore aziendale
- Informazioni su volume, validità e finalità d’uso dei dati da proteggere
- Tipologia di *use case* (es. dati in transito, dati inattivi, dati in elaborazione, firma digitale)
- Considerazioni tecniche e sulle minacce
- Tipi di crittografia attualmente in uso
- Componenti tecnici (ad es. *end-point*, reti, database, file server)
- Posizioni in cui esistono informazioni crittografiche (ad esempio DLL, hardware)
- Dipendenze tecniche (ad esempio dettagli sui componenti all'interno di questo caso d'uso che dipendono o si affidano ad altri sistemi per la propria sicurezza)
- Capacità di supportare algoritmi crittografici (pre e post-quantistici) simultaneamente

È possibile invece rimandare a una seconda fase la valutazione dei seguenti aspetti:

- scelta del miglior algoritmo da utilizzare;
- ordine o sequenza di ciò che deve essere aggiornato;
- percorsi alternativi alla quantum *remediation* (ad esempio, aggiornamento dell'intero sistema, cambio di paradigma).

È fortemente consigliato creare un archivio che implementi un modello gerarchico, che sia interrogabile e che tenga traccia delle relazioni/interazioni tra sistemi/oggetti diversi in modo tale da essere pienamente consapevoli di cosa viene impattato dall’eventuale cambio di un singolo item, sia esso un algoritmo, un certificato o altro.

8.2.4 *Plan*

A oggi non si dispone di tempistiche certe relativamente alla disponibilità del primo quantum computer in grado di compromettere la crittografia asimmetrica. Tuttavia, ci sono alcune stime indicative[153]:

- 2026: ≈14% di probabilità di violare l’algoritmo RSA-2048;
- 2031: ≈50% di probabilità di violare l’algoritmo RSA-2048;

[152] https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf

[153] Michele Mosca – University of Waterloo – Canada - https://cryptoexperts.com/awacs2016/slide-awacs2016/awacs-2016.pdf

- 2035: RSA-2048 non più sicuro.

Ciò è sufficiente a effettuare alcune prime considerazioni di massima: ad esempio, se un nuovo contratto di fornitura per sportelli automatici (ATM) prevede un ciclo di vita di dieci anni, e la sicurezza del firmware è basata su algoritmi classici, è evidente che sottoscriverlo comporta un potenziale rischio da gestire. Allo stesso modo, è necessario pianificare con maggiore attenzione l'emissione delle carte di credito in correlazione con la loro scadenza prevista, poiché si tratta di asset che, mediamente, rimangono in possesso del cliente dai tre ai cinque anni.

La prima azione utile per una corretta analisi del rischio è sfruttare quanto fatto nella fase precedente. Mediante il *crypto inventory* è possibile identificare hardware, software e servizi che fanno affidamento su algoritmi classici, i quali saranno conseguentemente valutati a rischio maggiore, soprattutto in relazione ai relativi tempi di sostituzione.

Una strategia a corredo, in tal senso, potrebbe essere quella di limitare la durata dei contratti di rinnovo, pur accettando una minor scontistica.

Generalmente, avendo a disposizione un *crypto inventory* sufficientemente esaustivo, l'analisi può essere svolta seguendo i seguenti passi principali:

- identificare la presenza degli algoritmi potenzialmente vulnerabili;
- comprendere i formati dei dati utilizzati, le interfacce delle applicazioni e delle librerie crittografiche per valutare le sostituzioni necessarie;
- individuare il miglior hardware che implementa le nuove strategie algoritmiche;
- identificare tutti i dispositivi di comunicazione che fanno uso di protocolli vulnerabili;
- identificare le dipendenze dei protocolli crittografici dalle caratteristiche degli algoritmi.

Va evidenziato che i nuovi algoritmi non potranno essere completamente equivalenti a quelli sostituiti. Infatti, potrebbero non condividere le stesse prestazioni o caratteristiche di affidabilità di questi ultimi a causa di molteplici fattori: differenze nelle dimensioni della chiave, della firma, nella gestione degli errori, del numero di fasi di esecuzione necessarie per eseguire l'algoritmo, della complessità del processo di creazione della chiave, ecc.

Questo determina che, una volta selezionati gli algoritmi sostitutivi, l'organizzazione dovrà sviluppare:

- un approccio basato sul rischio che tenga conto dell'impatto della sostituzione sull'operatività aziendale;
- un piano di migrazione, inclusivo di tempistiche e risorse necessarie;
- strumenti di convalida e verifica dell'implementazione;
- un aggiornamento capillare dei processi e delle procedure utilizzate da sviluppatori e utenti;
- un piano di comunicazione da utilizzare sia internamente che con i clienti e i partner esterni.

Il *crypto inventory* consente anche di capire quali sono i *vendor* di soluzioni e provider di servizi di cui bisogna preoccuparsi maggiormente, magari perché fornitori di PKI o HSM. Altra azione utile consiste nell'interrogare le proprie terze parti al fine di investigare il loro livello di consapevolezza

sul tema quantum, dando priorità anche in questo caso ai servizi/contratti ritenuti maggiormente critici.

In questa fase sarebbe utile creare all'interno della propria realtà un gruppo di lavoro eterogeneo dedicato al tema, che concorra a effettuare una pervasiva analisi dei rischi. Oltre alla funzione cyber security, tale gruppo potrebbe includere, ad esempio, personale dell'ufficio rischi, dell'ufficio acquisti e della compliance.

Un buon punto di partenza potrebbe essere l'ultima *Business Impact Analysis* effettuata, proprio al fine di iniziare le analisi dalle funzioni critiche e dai processi sistemici.

Per chiudere il cerchio, sarebbe opportuno porsi le seguenti domande:

- quali servizi si è pronti a sacrificare nel caso in cui non si fosse in grado di migrare tutte le applicazioni ad algoritmi post-quantum in tempo utile?
- quali piani di recovery è possibile implementare nel caso un quantum computer diventi disponibile a un attaccante e le applicazioni/servizi/hardware non siano migrate in tempo utile?
- come si può garantire la sicurezza dei dati (archivi e backup) qualora protetti da algoritmi classici divenuti nel frattempo obsoleti?

8.2.5 *Execute*

In questa fase si implementano le azioni di *remediation*, ovvero le attività definite all'interno del piano di trattamento del rischio definito nella fase precedente.

Tali attività possono riguardare l'utilizzo di soluzioni ibride o, se sufficientemente mature, l'utilizzo di soluzioni interamente post-quantum. Un aspetto a cui dare priorità è senz'altro orientare l'infrastruttura ad avere caratteristiche di *crypto agility*.

9 Bibliografia

Si suggerisce qualche testo per approfondire alcuni aspetti trattati sommariamente all'interno del resoconto.

Per una comprensione dell'affascinante mondo della meccanica quantistica (con capitoli dedicati a concetti alla base della computazione e della crittografia quantistica):

Gian Carlo Ghirardi: "Un'occhiata alle carte di Dio" – Il Saggiatore (Milano, 1997)

La "bibbia" del quantum *computing*:

Michael A. Nielse, Isaac L. Chuang: "Quantum Computation and Quantum Information" – Cambridge University Press (2010)

Per un panorama sempre aggiornato delle tecnologie quantistiche

https://www.oezratty.net/wordpress/2023/understanding-quantum-technologies-2023/ – *Sixth edition 2023 – Olivier Ezratty - Le Lab quantique*

Uno dei report di riferimento (*McKinsey&Company*) per la valutazione degli analisti, contenente diverse indicazioni:

https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf