UNIVERSITÀ DEGLI STUDI DI PADOVA

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

"DAL SILICIO AL QUBIT: STORIA, EVOLUZIONE E INNOVAZIONI QUANTISTICHE"

Relatore:

Prof. ENRICO ZANONI

Laureando:

ANDREA NALIN

Matricola: 2032449

ANNO ACCADEMICO 2023-2024

Data di Laurea: 27/09/2024

Indice

Introduzione

«La scienza non è nient'altro che una perversione se non ha come suo fine ultimo il miglioramento delle condizioni dell'umanità» - Nikola Tesla

1824, Stoccolma, Svezia: il chimico Jöns Jacob Berzelius nel suo laboratorio riscalda del fluorosilicato di potassio con altro potassio. Il prodotto era contaminato con siliciuro di potassio, decide quindi di mescolarlo con dell'acqua e rimuovere la contaminazione. Avviene la reazione e… ottiene il materiale del XXI secolo: il Silicio. Nemmeno Berzelius aveva idea della fantastica scoperta appena avvenuta.

Fin dall'antichità l'uomo ha sempre utilizzato materiali trovati in natura per procacciarsi cibo, combattere, costruire, evolversi. Dall'Età della Pietra, all'Età del Rame, passando all'Età del Bronzo e successivamente all'Età del Ferro. Arrivando fino al XXI secolo, dove il periodo è definito da molti come l'Età del Silicio.

Il Silicio non è un semplice semiconduttore, ma è il semiconduttore per eccellenza. Componente principale di materiali come vetro, ceramiche e cemento, il Silicio è importante per il suo utilizzo nella creazione di processori di dispositivi che utilizziamo tutti i giorni, direttamente o indirettamente. Dagli smartphone alla stazione spaziale internazionale, dai televisori alle antenne radio, dalle automobili agli aerei.

Ovunque ormai, è possibile vedere un dispositivo elettronico, il quale possiede un processore composto da Silicio. I processori sono paragonabili al cervello umano, eseguono calcoli e gestiscono le varie componenti. La componente fondamentale dei processori sono i transistor: piccoli apparecchi elettronici che gestiscono il flusso di corrente. I transistor posso avere dimensioni dai 3 cm, i quali sono utili che circuiti elettronici "più semplici", fino ai 3 nm. La dimensione dei transistor è cruciale per la realizzazione dei processori, perché da essi dipendono le performance e il consumo di energia, minore è la loro dimensione, migliore è la potenza di calcolo e la loro efficienza.

Qui sorge un problema: se i transistor sono troppo piccoli, il flusso di elettroni al loro interno può compromettere il passaggio di corrente e di conseguenza il corretto funzionamento del processore. Ed è proprio qui che entrano in gioco i computer quantistici, i quali sfruttando fenomeni complessi della fisica quantistica, permettono di ottenere una potenza di calcolo nettamente maggiore rispetto ai computer classici. La differenza alla base tra i 2 dispositivi sono le unità di informazione: i dispositivi che utilizziamo tutti i giorni possiedono come unità di informazione il bit che può assumere come valori 0 e 1, che corrispondono rispettivamente

all’assenza e presenza di corrente; Nei computer quantistici, il quanto di informazione fondamentale prende il nome di Qubit. A differenza dei bit utilizzati nei computer classici, i qubit possono assumere i valori 0 e 1, ma con una caratteristica unica: questi valori non sono limitati a uno stato esclusivo. In effetti, grazie ai principi della meccanica quantistica, un qubit può trovarsi in una sovrapposizione di stati, il che significa che può rappresentare simultaneamente sia lo 0 che l’1. In altre parole, un qubit può esprimere la presenza e l’assenza di corrente allo stesso tempo, un fenomeno che non ha equivalente nel mondo della computazione classica. Questa proprietà di essere in più stati contemporaneamente viene denominata sovrapposizione.

La sovrapposizione permette ai computer quantistici di elaborare simultaneamente un numero molto più grande di possibilità rispetto ai computer classici, che devono invece processare ogni stato in maniera sequenziale. Questo approccio consente ai computer quantistici di eseguire calcoli paralleli e simultanei su una scala che i computer classici non possono raggiungere, aprendo la strada a nuove frontiere nel campo della computazione e risolvendo problemi che, altrimenti, sarebbero insormontabili con le tecnologie tradizionali.

La scelta di questo argomento per la mia tesi è il risultato di una passione profonda e radicata per l’informatica, l’elettronica e la meccanica quantistica, discipline che da sempre mi affascinano per la loro complessità e il loro potenziale di trasformare il nostro mondo. Fin dai primi studi, il funzionamento dei computer e i principi che regolano la tecnologia digitale mi hanno incuriosito, stimolando un desiderio continuo di esplorare e comprendere a fondo le meccaniche dei dispositivi che utilizziamo tutti i giorni, sia in modo diretto che in modo indiretto. Le loro capacità e il loro limiti, nutrendo ancor di più il mio interesse sulla sfida del superamento di limiti che non avremmo mai pensato di raggiungere. Con il progredire della tecnologia, stiamo assistendo al raggiungimento di confini fisici che sembravano inarrivabili, soprattutto in termini di miniaturizzazione e velocità di elaborazione. Questa sfida mi ha spinto a indagare soluzioni innovative e a considerare come le nuove tecnologie, in particolare quella quantistica, possano superare tali barriere e aprire nuove possibilità nel campo dell’informatica. Inoltre, come appassionato fan dell’azienda Apple, ho sempre ammirato il lavoro che sta dietro ai loro processori, frutto di una continua ricerca di innovazione e superamento dei limiti tecnologici. Negli ultimi anni, Apple ha dimostrato un impegno straordinario nel portare avanti l’evoluzione dei propri chip, spingendosi costantemente oltre con processori sempre più potenti ed efficienti. Un esempio concreto di questa innovazione è il processore del Mac da cui sto scrivendo questa tesi, un prodigio tecnologico con ben 90 miliardi di transistor di soli 3 nanometri. È una sensazione unica e stimolante studiare proprio quei componenti che sto

utilizzando nell'esatto momento in cui ne esploro il funzionamento, rendendo l'esperienza di studio non solo teorica ma anche profondamente pratica e tangibile.

I. Storia ed evoluzione dei processori

In questo capitolo si intende esaminare l'evoluzione storica dei processori, ponendo particolare attenzione alla Legge di Moore, una delle previsioni tecnologiche più influenti nel settore dell'elettronica. Attraverso l'analisi di tale legge e delle sue implicazioni, si esploreranno i progressi compiuti nella microelettronica e il costante superamento dei limiti tecnologici, che hanno reso possibile lo sviluppo di processori sempre più potenti e compatti. Verranno inoltre discusse le tappe fondamentali che hanno segnato l'avanzamento dei processori, tracciando un collegamento tra le innovazioni del passato e le sfide future nel campo dei semiconduttori.

1.1. Legge di Moore

Nel 1965 Gordon Moore, cofondatore di Intel e Fairchild Semiconductor International, espose la tesi secondo la quale, nei successivi 10 anni il numero di transistor contenuti nei processori sarebbe raddoppiato di anno in anno, con un aumento minimo dei costi. Nel 1975 rivide la sua previsione affermando che il raddoppio sarebbe avvenuto ogni 2 anni. Nella figura 1.1 (grafico logaritmico) è possibile notare come l'affermazione di Moore sia corretta e come l'industria dei semiconduttori abbia seguito alla lettera le sue parole.

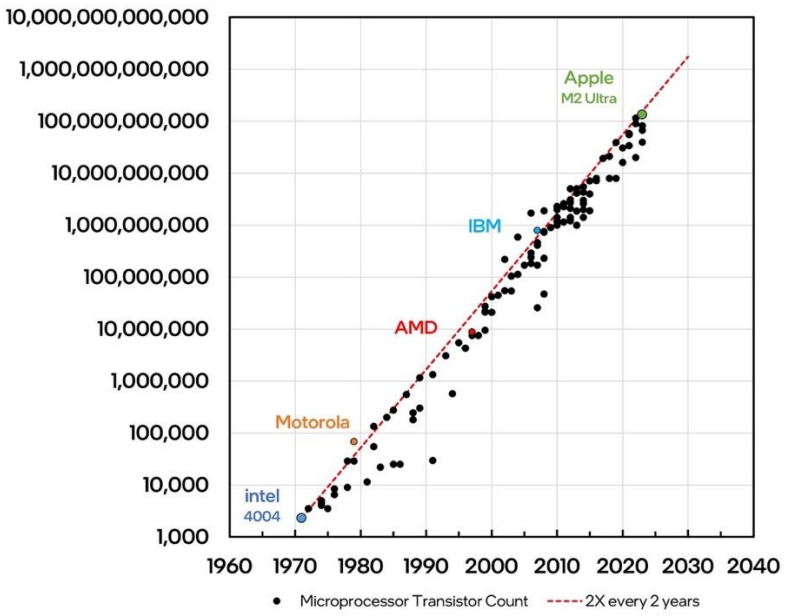

Figura 1: Numero di transistor presenti nei processori nel corso degli anni (grafico logaritmico) [1]

Esaminiamo ora se la Legge di Moore sia stata effettivamente rispettata nel corso degli anni. A tal fine, consideriamo due processori rappresentativi di epoche tecnologiche molto distanti: l'Intel 8080, rilasciato nel 1974, e l'Apple M1 Ultra, lanciato nel 2022. L'Intel 8080, prodotto un anno prima della revisione della Legge di Moore, contava 6.000 transistor, una quantità considerevole per l'epoca.
Per determinare se la crescita esponenziale prevista dalla Legge di Moore sia stata mantenuta, applichiamo la formula seguente:

$$X = 6000 \times 2^{\frac{N}{2}}$$

Dove:
- X è il numero previsto di transistor nel 2022.
- 6000 sono il numero di transistor dell'Intel 8080.
- N rappresenta il numero di anni trascorsi dal 1974 al 2022, ovvero 48 anni.

Calcolando il risultato, otteniamo una stima di circa 100.663.296.000 transistor per un processore equivalente nel 2022, se la Legge di Moore fosse stata seguita alla lettera.
Tuttavia, confrontando questo dato con la realtà, notiamo che il processore Apple M1 Ultra, rilasciato nel 2022, non si limita a contenere 100 miliardi di transistor, ma arriva a ben 114 miliardi di transistor. [2]
Questo significa che il progresso tecnologico non solo ha rispettato la previsione della Legge di Moore, ma l'ha addirittura superata. Il fatto che l'M1 Ultra conti 14 miliardi di transistor in più rispetto alla previsione dimostra come le innovazioni nell'ingegneria dei semiconduttori e nella miniaturizzazione dei componenti abbiano permesso di oltrepassare i limiti che Moore aveva ipotizzato, sottolineando così l'incredibile ritmo con cui la tecnologia continua ad evolversi.
Nel corso degli ultimi 60 anni in molti affermarono che la Moore's Law aveva i giorni contati, ma ogni volta che qualcuno affermava ciò, Apple, Intel o altre aziende nell'industria dei processori, trovavano un modo per dimostrare il contrario, innovando ulteriormente le proprie componenti.
L'affermazione di Moore era nata come un'osservazione empirica, cercando di prevedere lo sviluppo dei processori negli anni seguenti. Ma è diventata velocemente una vera e propria legge, al quale l'interno universo deve sottostare, come se fosse diventata la prima legge di Newton. Per Intel (leader per lo sviluppo di processori) quindi, diventa l'obiettivo da rispettare di anno in anno, mostrando al mondo come il proprio cofondatore avesse dettato una legge, che doveva essere rispettata correttamente. [3]

1.2. Il primo processore

Nel 1969 la Busicom (in precedenza Nippon Calculating Machine Corporation), azienda produttrice di calcolatrici, si rivolse a Intel per la creazione di una nuova calcolatrice computerizzata, tramite un set personalizzato di chip. Masatoshi Shima, che lavorava per l'azienda giapponese, propose ad Intel un sistema a 8 chip: 3 chip per interfacciarsi con le periferiche, un chip per la memorizzazione del codice del programma, un chip per i dati e gli ultimi 2 chip avrebbero costituito la CPU.

L'ingegnere di Intel, Ted Hoff, che si occupava delle trattative con Busicom però era preoccupato che la propria azienda non avesse le possibilità di produrre così tanti chip, soprattutto a causa dell'elevata richiesta di pin per l'interconnessione. Ciò avrebbe messo a dura prova i limiti della tecnologia di packaging in ceramica che Intel utilizzava al tempo. Per superare l'ostacolo, Hoff decise di proporre il dimezzamento del numero di chip, creando così il MCS-4. Sistema a 4 bit, costituito da un chip per la memoria del programma, chiamato 4001, un chip per la memoria dei dati (40 byte), il 4002, un chip per l'interfaccia delle periferiche, chiamato 4003, e infine un chip per la CPU, il 4004. In questo modo il problema del numero dei chip fu superato, anche grazie a Stanley Mazor, di Intel, che aiutò Hoff per le specifiche di ogni chip e per la loro produzione. Shima tornò in Giappone per implementare il software in modo che fosse adatto per il nuovo chip, e successivamente nel febbraio del 1970, ci fu l'accordo tra Intel e Busicom.

Tuttavia, ci furono diversi problemi nell'effettiva produzione di questi chip, infatti nessuno in Intel (nemmeno Hoff e Mazor) era capace di interpretare le specifiche e creare le corrispondenti reti logiche, a loro volta composte da porte logiche elementari. Questi diagrammi sono essenziali per la disposizione esatta dei vari transistor e delle altre componenti presenti nel chip fisico, senza di essi il processore non può essere sviluppato. A questo punto Intel non disponendo di progettisti, decide di fare una delle sue scelte migliori, assumendo l'ingegnere Federico Faggin, il quale aveva già sviluppato un computer da zero per Olivetti, in Italia.

In tutto questo la Busicom era all'oscuro dei problemi incontrati da Hoff e Mazor, e infatti quando Shima arrivò negli Stati Uniti per verificare che tutto andasse secondo i piani, si accorse che Intel era in ritardo con la scadenza del progetto. Allora Faggin elaborò un nuovo programma che potesse permettere a Intel di rispettare l'ormai vicina scadenza dell'accordo, e lavorando oltre 70 ore alla settimana, collaborando con Shima per la verifica della logica dei chip, Intel riuscì alla fine del 1970 a dare alla luce il primo processore della storia dell'umanità: l'Intel 4004.

Busicom deteneva però i diritti sul design e in questo modo poteva impedire a Intel la commercializzazione a terzi. Intel propose quindi, grazie alle pressioni da parte di Hoff, di ridurre il prezzo del chip per Busicom, acquisendo così il permesso di vendere il processore in tutto il mondo. Intel iniziò a pubblicizzare il 4004 tramite un annuncio che proclamava: *"Announcing a new era of integrated electronics."*, segnando così l'inizio di una vera e propria rivoluzione tecnologica. [4]

Figura 2: Intel 4004 [5]

1.3. L'evoluzione e il dominio dei mercati di Intel

Intel dopo la creazione del 4004 continua lo sviluppo dei suoi processori, proponendo la versione 8008, la quale però non soddisfa le aspettative del pubblico su larga scala, a causa di una grande presenza di bug, della difficile integrazione in un sistema, proprio perché richiedeva un elevato numero di componenti per l'integrazione, e della complessa architettura non facilmente programmabile.

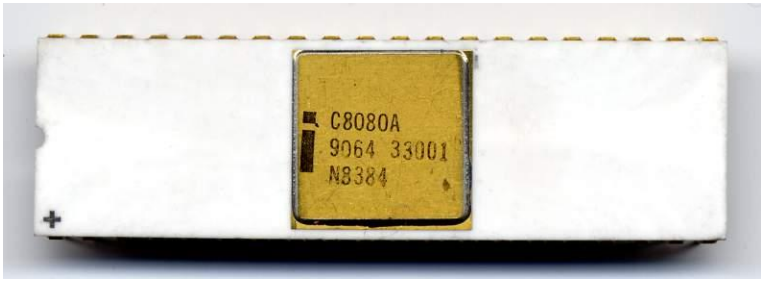

Figura 3: Intel C8080A [6]

Ciò spinse Federico Faggin, che fu fondamentale per lo sviluppo del 4004, a proporre il design innovativo dell'Intel 8080, il quale risultava essere un altro miracolo nel mondo dell'elettronica. Infatti, il nuovo processore aveva un design che lo distingueva nettamente dai suoi predecessori:

- Sette registri a 8 bit (A, B, C, D, E, H e L);
- Possibilità di combinazione di sei di questi registri per formare tre registri a 16 bit (BC, DE, HL);
- Stack pointer a 16 bit, in grado di indirizzare l'intera memoria disponibile;
- Indirizzamento indiretto della memoria tramite il registro a 16 bit (HL);
- Capacità limitata di eseguire operazioni a 16 bit;
- Indirizzamento delle 256 porte di I/O tramite uno spazio di indirizzamento riservato, senza occupare memoria;
- Bus dati a 8 bit e bus indirizzi a 16 bit, separati per una gestione efficiente del flusso di dati e indirizzi.

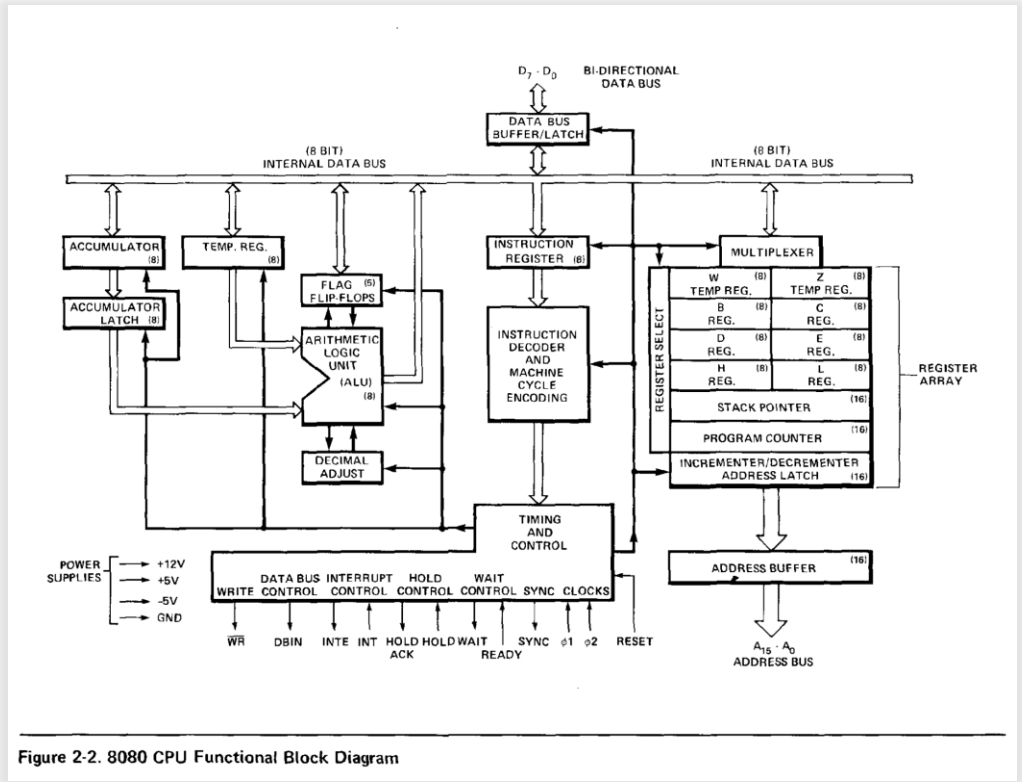

Figure 2-2. 8080 CPU Functional Block Diagram

Figura 4: Intel 8080 datasheet [7]

A differenza dei processori precedentemente sviluppati da Intel, l'8080 venne utilizzato in molti computer di quel periodo, come Altair 8800 della MITS (Micro Instrumentation and Telemetry Systems) e l'IMSAI 8080.

Figura 5: Altair 8800 [8]

Figura 6: IMSAI 8080 [9]

L'Intel 8080 grazie al suo design permetteva di semplificare notevolmente il layout delle schede madri, in questo modo necessitava di una logica minima rispetto ai sistemi più diffusi di quei tempi.

Inoltre, la capacità di eseguire operazioni a 16 bit, seppure poco frequenti, fu particolarmente apprezzato dai programmatori, permettendo loro uno sviluppo di programmi più complessi e articolati.

Ma il vantaggio principale rimase comunque essere i pionieri del settore. Infatti, Intel essendo stata la prima a esplorare questo nuovo mercato, divenne facilmente leader, dominando così il mercato.

Successivamente Intel continuò il perfezionamento del 8080 sviluppando una versione migliore, l'Intel 8085, l'8086 e l'8088, fondamentali per l'aggiornamento delle architetture dei processori. [7]

1.4. L'Architettura x86

Dopo il grandissimo successo dell'8080, Intel doveva continuare ad affermarsi sul mercato proponendo processori sempre più innovativi, per portare allo step successivo le sue componenti elettroniche e rispettare la Legge di Moore. Decise quindi di iniziare lo sviluppo dell'Intel 8086, con alcune grandi differenze. La prima sono il numero di pin, che passano da 8 a 16, e la seconda avrebbe permesso a Intel di rivoluzionare il mondo dell'informatica ancora una volta: l'Architettura x86.

Questa architettura è tutt'oggi utilizzata nella maggior parte dei dispositivi elettronici (sebbene le cose negli ultimi anni stiano un po' cambiando) e molto probabilmente il dispositivo utilizzato per la lettura di questa tesi è un dispositivo che usa l'architettura inventata da Intel nel 1978.

L'x86 è una famiglia di architetture di set di istruzioni per computer con set di istruzioni complesso (CISC), il cui nome deriva dai successori dell'8086 i quali terminavano tutti con "86": Intel 80186, l'80286, l'80386 e l'80486. Negli anni '80 e '90, il termine x86 sostanzialmente corrispondeva alle CPU compatibili con l'8086. Nell'età moderna invece si riferisce alla compatibilità binaria con i set di istruzione a 32 bit che l'80386 possiede, proprio perché il set di istruzioni è ampiamente utilizzato ai giorni nostri. Infatti, questa architettura è presente nella stragrande maggioranza dei dispositivi, dai PC ai laptop, dai server alle workstation; di conseguenza la maggior parte dei software sviluppati, si basano sull'x86. Negli anni Intel provò a sostituirla con architetture più "eleganti", come l'iAPX 432 e l'Itanium, ma essa prevalse sulle altre grazie ai continui miglioramenti e alla sua scalabilità, dimostrando come la costante evoluzione possa mantenere rilevante una tecnologia anche di fronte alla concorrenza di nuove soluzioni. [10]

1.5. Le architetture a 32 e 64 bit

Successivamente allo sviluppo dell'architettura x86, Intel decise di creare un nuovo design dei processori. Negli anni '80, i chip a 16 bit iniziarono ad essere limitanti sotto alcuni aspetti: lo sviluppo di software e la gestione dei dati. Questi processori possedevano una memoria che si limitava a 64 KB, che inizialmente era sufficiente per l'esecuzione dei programmi dell'epoca, ma con il passare degli anni, sebbene si iniziarono a utilizzare tecniche per aggirare questo problema (come la segmentazione utilizzata nell'Intel 8086), lo sviluppo software ne iniziava a risentire. Una memoria limitata non permette la creazione di programmi complessi, i quali necessitavano di sempre più risorse per un corretto funzionamento. [11]

Intel intraprese quindi lo sviluppo di una nuova generazione di processori, mantenendo sempre l'incredibile architettura x86 come base ma ampliandola da 16 bit a 32 bit, compiendo per l'ennesima volta una svolta nel mondo dell'informatica. Con questa nuova introduzione, consentì di passare dai 64 KB di memoria, ai 4 GB di RAM, una quantità impensabile per l'epoca. Ciò permise lo sviluppo di software molto più complessi e articolati, i quali potevano usufruire di maggiore memoria, e di conseguenza ampliare ulteriormente il mercato di vendita, andando a soddisfare una parte sempre più grande della popolazione. [12]

Nel 1985, quindi, Intel introduce l'80386, il quale non solo possedeva maggiori performance rispetto ai suoi predecessori a 16 bit, ma era pure retrocompatibile con il software esistenze, e ciò facilitò notevolmente la transizione degli sviluppatori e degli utenti, al nuovo dispositivo. Questa compatibilità contribuì alla rapida diffusione del nuovo processore, e l'architettura a 32 bit divenne presto lo standard de facto per i personal computer.

Negli anni 90 l'80386 e i suoi successori, giocarono un ruolo importante per la diffusione del World Wide Web, il quale richiedeva computer sempre più potenti per supportare la grafica web, il multimedia e il networking.

Ciò che stava alla base di questo notevole miglioramento, era che il chip possedeva un bus dati a 32 bit, ciò permetteva al processore di trasferire blocchi di dati più grandi in un singolo ciclo di clock, migliorando significativamente le prestazioni. L'elaborazione di blocchi di dati maggiori permise un utilizzo più fluido e dinamico dei vari software, soprattutto nei settori del gaming, dell'elaborazione di video e delle simulazioni. [13]

L'architettura rimase dominante fino agli inizi del 2000, quando l'industria iniziò lo sviluppo di processori a 64 bit, per affrontare l'ulteriore complessità dei software che di anno in anno aumentava. Tuttavia, l'architettura segnò l'industria dell'informatica e tutt'oggi molti software sono compatibili anche con un'architettura creata 40 anni fa, ciò dimostra come uno sviluppo accurato e flessibile possa portare allo sviluppo di architettura che sono "difficili" da dimenticare, e che i loro vantaggi sono rimasti duraturi nel tempo.

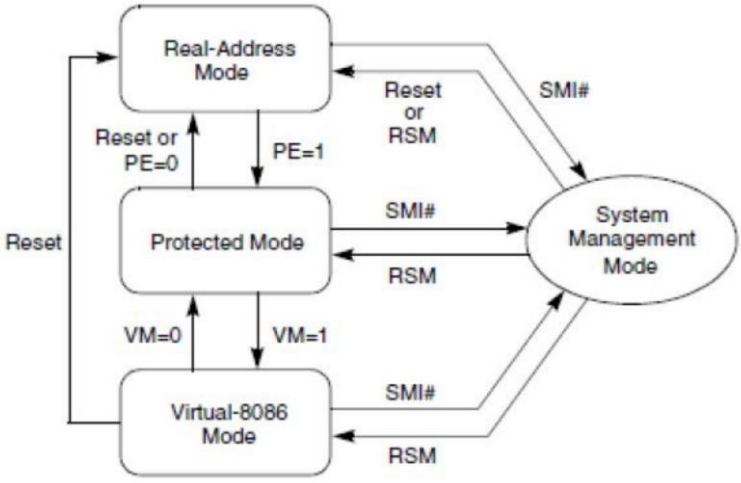

Figura 7: 32-bit architecture [14]

Il successivo passaggio dall'architettura a 32 bit a quella a 64 bit non differiva molto rispetto al passaggio dai 16 bit fino ai 32 bit, ciò che si voleva mantenere era la retrocompatibilità, portando però un incremento significativo delle performance.

I problemi maggiori furono appunto mantenere la compatibilità con i modelli precedenti, specialmente la specifica delle dimensioni del dato da trasferire, se erano dati ad 8, 16, 32 o 64 bit. Inoltre, ciò comportava alla considerazione di un nuovo modello di memoria, portando un utilizzo più fluido dei dispositivi.

Ciò che venne fatto dalle varie aziende del tempo (perché oltre ad Intel arrivarono anche aziende come AMD a far parte del settore) fu quello di:

1. Introdurre una nuova modalità operativa, la quale era compost da due sotto-modalità: Compatibility mode e 64-bit mode.
2. Passare al modello di memoria lineare nella sotto-modalità a 64 bit
3. Mantenere invariato il formato delle istruzioni, aggiungendo un nuovo prefisso per utilizzare i registri a 64 bit.

Tutte gli obiettivi furono rispettati e infatti venne sviluppato un nuovo modo di gestione dei dati, chiamato x32e, il quale era composto da 2 modalità:

- 64-bit mode: permette l'utilizzo di applicazioni che richiedono 64 bit appunto, portando così il numero di registri utilizzati da 8 a 18.
- Compatibility mode: permette quello che gli utenti di tutto il mondo richiedevano, cioè la possibilità di utilizzare software a 16 o 32 bit senza problemi o incompatibilità, evitando di dover aspettare una nuova versione delle applicazioni.

Grazie a questa nuova introduzione e altri piccoli miglioramenti, si iniziarono a diffondere a livello globale, nei primi anni del 2000 computer che utilizzavano questa nuova architettura.

L'espansione di questo nuovo design fu rapida e tutt'oggi la maggior parte dei personal computer fa ancora utilizzo di questa architettura.

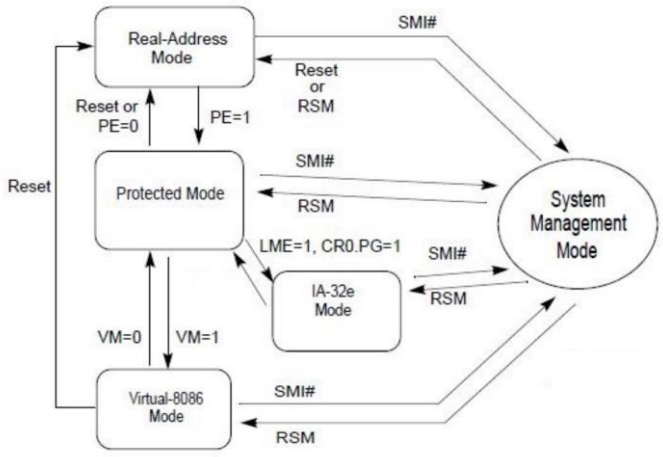

Figura 8: 64-bit architecture [14]

Nelle due immagini è possibile vedere le architetture a 32 bit (a sinistra) e a 64 bit (a destra). Ciò che le distingue tra loro è la presenza della IA-32e Mode appena descritta, che permette la gestione di dati da 8, 16 e 32 bit. È possibile notare inoltre l'elemento "Virtual-8086 Mode" il quale corrisponde a quella parte dell'architettura che permette la retrocompatibilità con i dispositivi a 16 bit (l'Intel 8086 per esempio). [14]

1.6. Processori multicore

Fino al 2005, la maggior parte dei processori presenti sul mercato erano single-core, cioè processori composti da una singola unità di elaborazione. In quegli anni, questa configurazione era sufficiente per supportare lo sviluppo software e garantire un utilizzo fluido dei dispositivi. Tuttavia, con il tempo, l'aumento delle richieste di risorse da parte dei programmi, come RAM e potenza di calcolo, ha messo in evidenza i limiti di questi processori. Le tecnologie disponibili a quel tempo permettevano solo incrementi marginali delle prestazioni, per esempio, attraverso l'introduzione della tecnologia Hyper-Threading con il Pentium 4 Northwood di Intel, che simulava la presenza di due core logici per migliorare il multitasking e la reattività. Inoltre, furono incrementate le dimensioni della cache e migliorata l'efficienza delle microarchitetture, cercando di aumentare la frequenza di clock.

Tuttavia, c'era un limite fondamentale: la potenza dissipata dai processori è proporzionale alla frequenza di clock, e superando una certa soglia (generalmente tra 2 e 3 GHz), la potenza dissipabile non può superare i 100-150 W senza provocare surriscaldamento. Questo limite termico impedisce di aumentare ulteriormente la frequenza di clock, segnando così il punto di arresto della crescita delle prestazioni nei processori single-core.

Per superare questo ostacolo, Intel e AMD optarono per una nuova architettura: quella dual-core, che puntava sul parallelismo per migliorare le prestazioni. Le due aziende fornirono ai sistemi operativi una configurazione simile a quella dei sistemi multiprocessore tradizionali, introducendo processori con due unità di elaborazione separate. Nonostante ciò, all'inizio, molti software non erano ottimizzati per sfruttare questa nuova architettura, con il risultato che spesso uno dei core rimaneva inutilizzato. Con il tempo, gli sviluppatori hanno adattato il software per sfruttare appieno le potenzialità delle architetture multicore, riconoscendone i notevoli vantaggi in termini di prestazioni. [15]

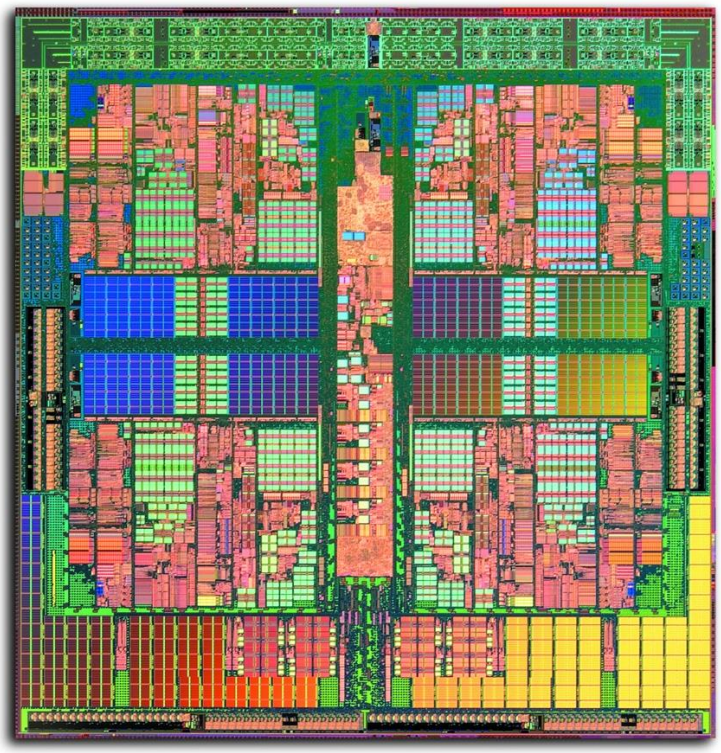

Figura 9: AMD Opteron quad-core processor [16]

I vantaggi dei processori sono molti, ma quello che salta immediatamente all'occhio con il semplice utilizzo di essi è l'aumento di capacità di elaborazione. È come se ogni core fosse un processore a sé stante che viene sfruttate dal sistema operativo o dalle diverse applicazioni. Per esempio, in un server virtualizzato, ogni virtual machine (VM) ha la capacità di utilizzare uno o più core virtualizzati, permettendo così alle VM di coesistere e cooperare simultaneamente su un server fisico. Se invece ci spostiamo sull'ambito software, essi sono in grado, se ottimizzati in maniera corretta, di sfruttare a pieno il parallelismo e utilizzare di conseguenza diversi core per aumentare notevolmente le prestazioni, impossibili da raggiungere con sistemi single-core. Sebbene i core siano distinti tra loro, le altre componenti vengono condivise per far cooperare al meglio l'insieme dei chip, per esempio i bus interni, cache del processore.

Ciò risulta essere un grande vantaggio solo se effettivamente sfruttato, se i sistemi operativi o i vari software non sfruttano a pieno i diversi core, si ha l'effetto opposto, cioè una riduzione notevole delle performance, perché tutta l'elaborazione dei dati viene fatta su un singolo core, e ciò comporta a degli importanti svantaggi. Inoltre, i processori multicore necessitano un grande quantitativo di energia, che negli ultimi anni ha rallentato molto il loro sviluppo, perché sebbene le performance aumentassero, la loro efficienza crollava a picco, portando anche problemi come il surriscaldamento dei chip. [17]

Nel corso degli anni, i processori multicore hanno visto una rapida evoluzione, con Intel e AMD che si sono affermate come i principali protagonisti del settore. Sebbene i vari processori

ricevessero un costante aumento delle prestazioni negli anni, il focus di queste aziende è stato spesso orientato più sul profitto delle vendite che sull'ottimizzazione del consumo energetico e dell'efficienza complessiva. Nel 2020, l'introduzione della linea di processori Apple Silicon ha però segnato un punto di svolta significativo, spingendo Intel e AMD a rivalutare le loro priorità e a sviluppare processori che non solo offrono elevate performance, ma anche una maggiore efficienza, riducendo il consumo energetico. [18]

1.7. La rivoluzione dell'intelligenza artificiale

Negli ultimi anni si è visto un notevole interesse nei confronti dell'intelligenza artificiale, partendo da OpenAI che diffonde ChatGPT, fino ad Apple che annuncia Apple Intelligence; ma cos'è l'IA?

L'Artificial Intelligence non è altro che un ramo dell'informatica che si occupa dello sviluppo di sistemi capaci di svolgere compiti che, in genere, richiedono l'intelligenza umana. Per esempio, il riconoscimento di immagini, compressione del linguaggio naturale, l'apprendimento automatico e l'elaborazione di decisioni. Quindi, l'IA consiste nel simulare l'intelligenza umana tramite algoritmi sofisticati e specifici per determinati problemi. Il machine learning, per esempio, consiste nell'apprendimento di dati tramite algoritmi che automaticamente migliorano l'utilizzo di questi nuovi software. Una sua sottocategoria è il deep learning che sfrutta le reti neurali profonde, cioè strutture ispirate al cervello umano, per il riconoscimento di schemi piuttosto complessi in grandi quantità di dati. L'IA ai giorni nostri è integrata in molte delle tecnologie che si utilizzano quotidianamente, come le raccomandazioni di prodotti sugli e-commerce, la gestione delle risorse presenti nei cloud, o l'analisi dei big data in contesti scientifici e aziendali. Nei prossimi anni non farà altro che insiedarsi ancora di più nella vita di tutti i giorni.

Ciò che però risulta molto interessante è l'applicazione dell'intelligenza artificiale nel campo dei processori. Oltre alle classiche unità di calcolo come CPU e GPU (sfruttate per il calcolo avanzato di immagini), sono state sviluppate anche processori specifici per l'utilizzo di AI: le NPU (Neural Processing Unit).

Le NPU sono componenti hardware specializzate, progettati appositamente per l'esecuzione di algoritmi di deep e machine learning, che permette ai dispositivi la gestione di calcoli complessi richiesti dalle reti neurali. Anche CPU e GPU possiedono le capacità per l'elaborazione di questi calcoli, ma l'utilizzo di architettura specifiche come le NPU offre vantaggi significativi dal punto di vista delle performance e dell'utilizzo di risorse (come il consumo energetico).

In particolare, le NPU sono ottimizzate per eseguire operazioni di matrici, convoluzioni e altri calcoli comuni nell'ambito delle reti neurali, e ciò lo fanno in maniera più efficiente rispetto ai classici processori. Infatti, le Neural Processing Unit sono specificatamente progettate per l'esecuzione di operazioni parallele di massa, riducendo al minimo le tempistiche e il consumo energetico per l'elaborazione di tali operazioni. Ciò permette di processare grandi volumi di dati in tempi ridotti, risultando particolarmente abiti negli ambiti del riconoscimento facciale, dell'elaborazione del linguaggio naturale, e della guida autonoma. Una volta implementata l'architettura NPU in un sistema, le altre componenti come CPU e GPU possono gestire i compiti tradizionali, come l'elaborazione delle istruzioni del sistema operativo, in questo modo si evitano rallentamenti o i classici colli di bottiglia causati dall'elaborazione di grandi quantità di dati, portando così ad una maggiore efficienza a tutto il sistema. [19]

Negli ultimi anni molte aziende hanno iniziato a sviluppare i loro NPU, tra cui Apple, la quale ha annunciato nel 2017 l'introduzione nei suoi processori del Neural Engine, a partire dall'A11 Bionic. Esso fu specificatamente ottimizzato per compiti che potevano risultare complessi per la CPU, come il riconoscimento facciale con il Face ID, la realtà aumentata, e la fotografia computazionale, migliorando così l'esperienza utente in modo tangibile. Infatti, l'NPU di Apple permette di eseguire miliardi di calcoli al secondo, consentendo così il rapido riconoscimento facciale e l'elaborazione avanzata di immagini in tempo reale. Questa nuova introduzione, oltre ai vantaggi più tangibili, ha aperto nuove possibilità per gli sviluppatori, consentendo così uno sviluppo di applicazioni più avanzate e ricche di funzionalità basate sull'intelligenza artificiale. Apple ha anche rilasciato strumenti di sviluppo come Core ML, che consentono di sfruttare facilmente il Neural Engine nelle applicazioni, semplificando così l'integrazione dell'IA nelle app iOS. [20]

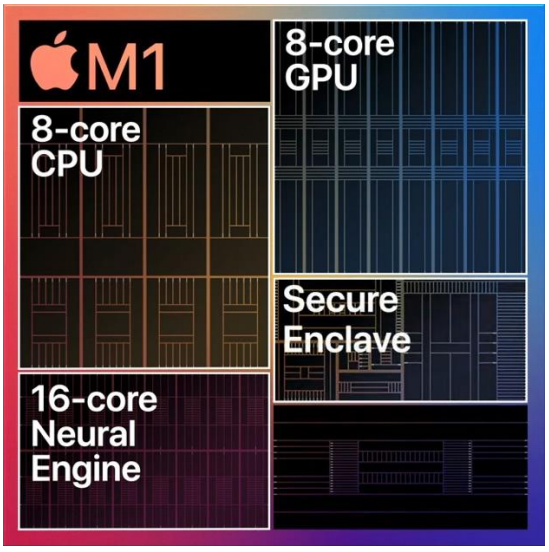

Figura 10: Processore Apple M1 [21]

D’altra parte, abbiamo le TPU (Tensor Processing Unit) sviluppate negli ultimi anni dal colosso di Google, le quali hanno lo stesso scopo delle NPU, cioè la specializzazione nei campi del machine learning e del deep learning. Tuttavia, hanno una particolare differenza che le distinguono dalle NPU, cioè l’architettura con cui vengono costruiti. Infatti, le NPU seguono il classico design di Von Neumann, secondo la quale le varie componenti hardware come il processore, memoria e input/output sono separate tra loro. Le TPU invece sono basate su un’architettura chiamata Systolic Array Architecture, che integra la memoria direttamente all’interno del processore su un unico chip. In questo modo il processore ha la capacità di eseguire l’elaborazione di dati in modo parallelo e più efficiente rispetto alle normali architetture. Dal punto di vista delle applicazioni invece, le NPU sono nate per essere integrate nei dispositivi consumer, come smartphone, tablet e computer, e sono ottimizzate per eseguire in modo rapido operazioni di intelligenza artificiale direttamente sull’hardware dell’utente. D’altro canto, invece le TPU sono state ideate inizialmente per l’uso nei data center di Google, dove vengono utilizzate per eseguire calcoli su vasta scala necessari per addestrare modelli di machine learning complessi, come per la classica ricerca su Google, la traduzione automatica, e i suggerimenti presenti su YouTube.

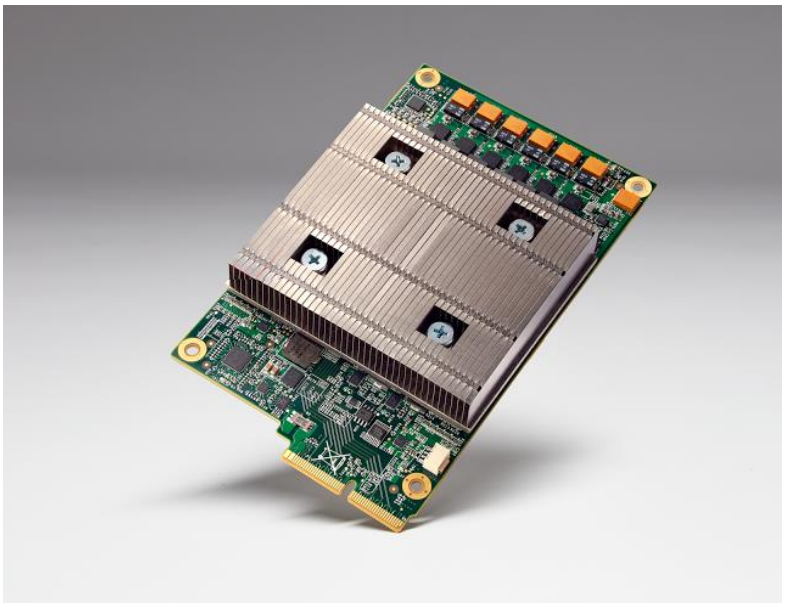

Figura 11: Tensor Processing Unit di Google [22]

In generale, l’industria tecnologica sta progressivamente spostando l’attenzione verso lo sviluppo di nuovi tipi di processori specializzati in ambiti specifici, come l’intelligenza artificiale e la grafica avanzata. Questo perché si sta piano piano sviluppando una crescente consapevolezza che non è più sufficiente concentrare tutte le risorse sul miglioramento delle

CPU tradizionali, le quali, sebbene versatili e in grado di gestire un ampio spettro di applicazioni, non possono competere in termini di efficienza e prestazioni con unità progettate per compiti specifici. Le varie varianti delle CPU come le NPU per l'intelligenza artificiale, le GPU per la grafica e i calcoli paralleli, e le TPU per l'apprendimento automatico, sono progettate per ottimizzare compiti specifici e offrono prestazioni superiori in questi contesti rispetto alle CPU generiche. In questo modo, i classici processori non sono impegnati in ambiti che possono svolgere altre componenti, e consentendo loro una gestione migliore delle operazioni generali. Ciò non significa che lo sviluppo delle CPU verrà abbandonato, ma piuttosto che si stanno creando ecosistemi di processori diversificati, in cui ogni componente svolge un ruolo ottimizzato per specifiche funzioni, contribuendo così ad un sistema complessivo più potente ed efficiente. [23]

1.8. Limiti dei processori moderni e le prospettive future

Dal 1971, anno in cui Intel lanciò l'iconico 4004, fino al 2024 con l'annuncio del processore Apple M4, gli Intel Lunar Lake e la serie Ryzen 9000 di AMD, i processori hanno subito un'evoluzione esponenziale. Questa evoluzione ha trasformato l'esperienza quotidiana delle persone di tutto il mondo, permettendo ad esse di svolgere le operazioni più semplici come una ricerca su Google, fino allo sviluppo di applicazioni software complesse e di alto livello. Tuttavia, nonostante questi progressi straordinari e i futuri sviluppi, i processori basati sul silicio stanno raggiungendo i loro limiti intrinseci. Negli ultimi anni soddisfare la legge di Moore è risultato sempre più difficile, a causa delle crescenti sfide tecnologiche e fisiche legate alla miniaturizzazione dei transistor e alla gestione del calore.

Una delle sfide più significative è la continua riduzione delle dimensioni dei transistor. I quali negli anni hanno subito un'incredibile miniaturizzazione portando incredibili miglioramenti in termini di prestazioni ed efficienza energetica, ma ciò comporta anche numerosi problemi tecnologici. Tra questi, vi è il limite fisico della miniaturizzazione: man mano che i transistor si avvicinano alla scala atomica diventa sempre più difficile controllare il comportamento degli elettroni, che possono attraversare le barriere isolanti. Questo fenomeno chiamato Tunneling quantistico, provoca flussi di corrente indesiderati e compromette la corretta funzionalità del processore, riducendone così l'affidabilità.

Un'altra problematica critica è la gestione termica. Con la riduzione delle dimensioni dei transistor aumenta la densità dei dispositivi sui chip, che a sua volta rende più complessa la

dissipazione del calore generato. La difficoltà nel raffreddare adeguatamente i chip può portare a temperature operative elevate, accelerando così l'usura delle componenti e riducendo la loro durata nel tempo. Questo effetto, noto come "Thermal runaway", può compromettere le prestazioni e la longevità dei processori. [24]

Infine, lo sviluppo di transistor sempre più piccoli comporta costi crescenti. Ogni riduzione nelle dimensioni richiede enormi investimenti in ricerca e sviluppo, e l'adozione di nuove tecnologie di produzione come la litografia EUV. Con l'aumento della complessità, i costi di produzione aumentano esponenzialmente, rendendo la creazione di nodi più piccoli finanziariamente impegnativa per i produttori. [25]

In conclusione, i processori basati sul silicio hanno rappresentato una pietra miliare nello sviluppo tecnologico e continueranno a essere fondamentali per molti anni a venire, con ulteriori sviluppi che nei prossimi anni vedremo, come i processori 2D, materiali alternativi al silicio, e i transistor a nanofili all'orizzonte. Nonostante ciò, non significa che bisogna limitarsi a questi tipi di processori, e attendere i piccoli miglioramenti che avvengono di anno in anno, ma bisogna anche dare uno sguardo al futuro ed esplorare nuove innovazioni, come il quantum computing e i processori ibridi, che potrebbero rappresentare il prossimo grande salto nell'evoluzione dei processori.

II. Calcolatori Quantistici

I computer quantistici rappresentano una rivoluzione nel modo di elaborare l'informazione, poiché sfruttano i principi della meccanica quantistica invece della fisica classica che governa i computer tradizionali. La differenza fondamentale tra i computer classici e quelli quantistici risiede nel concetto di bit e qubit.

Da una parte un bit classico può assumere solo due stati definiti, 0 o 1, ed è l'unità fondamentale di informazione per i computer tradizionali. D'altra parte, un qubit è un'unità di informazione che sfrutta due importanti proprietà quantistiche: la sovrapposizione e l'entanglement, le quali permettono al qubit una connessione intrinseca e una potenza di calcolo non paragonabile a quella dei processori in silicio. [26] [27]

Grazie a questa differenza strutturale, i computer quantistici possono eseguire maggiori operazioni contemporaneamente permettendo a problemi come la fattorizzazione di grandi numeri, che richiederebbero migliaia di anni per essere risolti da un computer classico, di essere risolti in pochi minuti da un computer quantistico. [28]

Tuttavia, il mondo della meccanica quantistica è estremamente delicato. I qubit sono molto sensibili alle interferenze esterne e richiedono condizioni di funzionamento estremamente specifiche, come temperature vicine allo zero assoluto e ambienti privi di vibrazioni. La sfida tecnologica di costruire computer quantistici stabili e scalabili è attualmente uno degli ostacoli principali al loro sviluppo su larga scala. [29]

Sebbene i computer classici continueranno a essere fondamentali per molte applicazioni e per i problemi di tutti i giorni, i computer quantistici offrono nuove possibilità per risolvere problemi complessi che i sistemi tradizionali non possono affrontare, con il potenziale di trasformare radicalmente settori come la crittografia, l'ottimizzazione e la simulazione di fenomeni fisici. [30] [31]

2.1. I principi della meccanica quantistica

Nella meccanica quantistica, i concetti di sovrapposizione, entanglement e l'interferenza quantistica sono alla base del funzionamento dei computer quantistici, i quali offrono possibilità di calcolo nettamente superiori rispetto ai computer classici. Questi fenomeni quantistici permettono ai qubit di elaborare informazioni in modo completamente diverso rispetto ai bit classici, aprendo nuovi orizzonti nella risoluzione di problemi complessi.

2.1.1. Sovrapposizione

La sovrapposizione è un fenomeno fondamentale della meccanica quantistica, che descrive lo stato di una particella o sistema quantistico che esiste simultaneamente in più stati possibili. Questo fenomeno permette ad un oggetto di trovarsi contemporaneamente in due stati differenti; differenza sostanziale della meccanica classica dove un oggetto può essere in un solo stato in un dato momento. La sovrapposizione degli stati è possibile fino ad un determinato momento, cioè quando avviene la misurazione del sistema.

Il fenomeno è descritto matematicamente tramite le funzioni d'onda, le quali rappresentano le probabilità associate a ciascuno stato. Una volta che avviene la misurazione, la funzione d'onda di ogni singolo stato "collassa", determinando come risultato uno dei due stati sovrapposti.

Questo fenomeno viene sfruttato nel calcolo quantistico dai qubit, i quali fino alla misurazione del loro stato, corrispondono simultaneamente sia allo 0 che all'1. [32] [33]

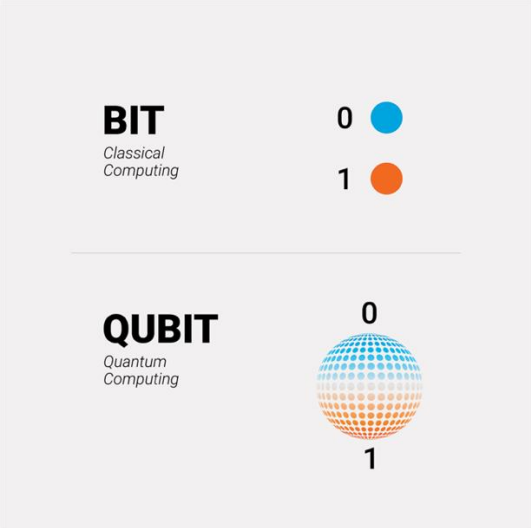

Figura 12: Rappresentazione di un bit e di un qubit [34]

2.1.2. Entanglement

L'entanglement è un fenomeno quantistico che si verifica quando due o più particelle diventano strettamente correlate, in modo tale che lo stato di una particella non possa essere descritto in modo indipendente rispetto allo stato dell'altra, anche se le particelle sono separate da grandi distanze. Indipendentemente da quanto distano, la modifica dello stato di una delle particelle, influirà istantaneamente sull'altra. Ciò può sembrare che violi le leggi della relatività secondo la quale il passaggio di informazione avviene in modo più rapido rispetto alla velocità della luce. Ma non è così. Infatti, l'entanglement non comporta

un vero e proprio trasferimento diretto di informazioni, perché non c'è uno scambio di segnali tra le due particelle entangled, ma lo stato di una particella "rivela" automaticamente lo stato dell'altra senza aver bisogno di una comunicazione diretta. Questo fenomeno viene sfruttato nei qubit per creare correlazioni tra stati quantistici che permettono l'elaborazione simultanea di informazioni distribuite su più qubit, migliorando così l'efficienza dei calcoli. [35] [36] [37]

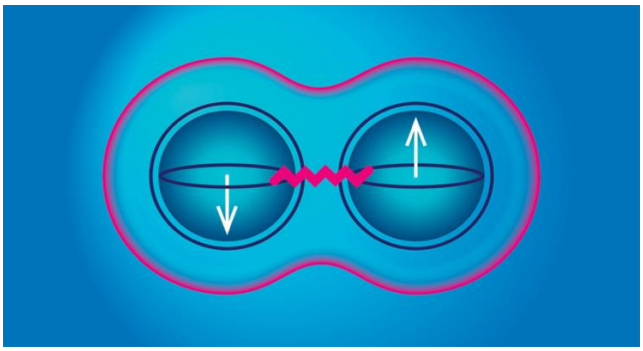

Figura 13: Rappresentazione del fenomeno dell'Entanglement [34]

2.1.3. Interferenza quantistica

Quando onde associate a particelle quantistiche, come elettroni o fotoni, si sovrappongono, si verifica il fenomeno chiamato: interferenza quantistica. Proprio come le onde dell'acqua, queste onde quantistiche possono interferire tra di esse in modo costruttivo e distruttivo. Nel caso di interferenza costruttiva, le varie onde si sommano tra di loro amplificando l'intensità complessiva. D'altra parte, l'interferenza distruttiva avviene quando più onde si annullano reciprocamente, riducendo o eliminando del tutto l'intensità in alcune regioni.
A differenza delle particelle nella meccanica classica, le quali seguono delle traiettorie ben definite, le particelle quantistiche possono essere descritte da una funzione d'onda che rappresenta la probabilità di trovare la particella in un determinato luogo. Una volta che due onde si sovrappongono tra di esse, avviene il fenomeno dell'interferenza. Essa viene sfruttata dai computer quantistici per l'amplificazione delle probabilità desiderate e la cancellazione di quelle indesiderate. [38]

L'applicazione della meccanica quantistica ai computer permette non solo una potenza computazionale esponenzialmente superiore, ma anche un modo completamente nuovo di affrontare i problemi. Mentre nei computer classici la logica si basa su stati binari definiti, i computer quantistici operano in un regno probabilistico, in cui l'informazione viene elaborata sfruttando la natura incerta e non intuitiva del mondo quantistico. Ciò presenta dei pro e dei

contro, per esempio, l'algoritmo di Shor mette in crisi dati crittografici basati sulla complessità della fattorizzazione. Se questo algoritmo fosse disponibile su scala mondiale, permetterebbe di accedere ad informazioni crittografate in maniera pressoché immediata.

2.2. Qubit: Il fondamento del calcolo quantistico

Il qubit, o bit quantistico, è l'unità fondamentale della computazione quantistica, un concetto che ridefinisce le fondamenta della tecnologia di calcolo rispetto ai bit classici dei computer tradizionali. Introdotto da Benjamin Schumacher, il qubit è la controparte quantistica del bit binario, ma con la capacità di esistere non solo negli stati di 0 e 1, bensì in una sovrapposizione quantistica di entrambi gli stati. Questa proprietà consente ai qubit di processare un numero maggiore di informazioni simultaneamente rispetto ai bit classici, permettendo una gestione e risoluzione di problemi troppo complessi o quasi impossibili da eseguire per i computer tradizionali.

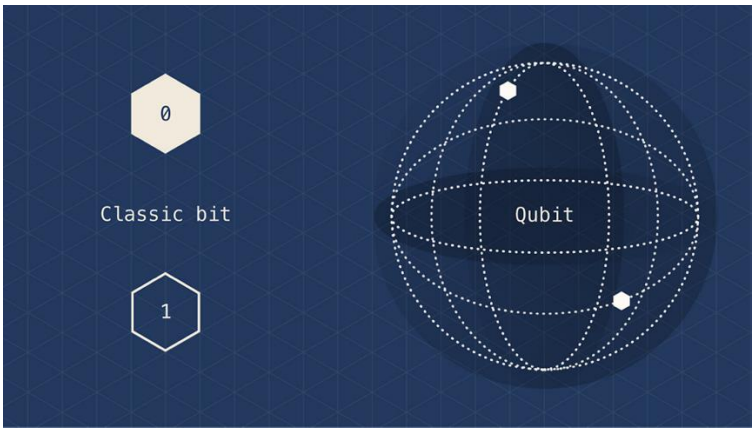

Figura 14: Rappresentazione del bit binario e del qubit [39]

La rappresentazione matematica del qubit descrive lo stato quantistico di un qubit, che si trova in una sovrapposizione degli stati base $|0\rangle$ e $|1\rangle$, la cui equazione è:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Dove $|\psi\rangle$ indica lo stato del qubit, $|0\rangle$ e $|1\rangle$ indicano gli stati base del qubit, analoghi a 0 e 1 nei bit classici, infine α e β sono coefficienti complessi che rappresentano le ampiezze di probabilità associate rispettivamente agli stati $|0\rangle$ e $|1\rangle$.
Una delle proprietà fondamentale del qubit è lo spin che deriva direttamente dalla meccanica quantistica e gioca un ruolo cruciale nel suo funzionamento. Lo spin di una particella

quantistica, come un elettrone, può essere immaginato come una sorta di "rotazione" intrinseca, anche se non corrisponde esattamente a un movimento fisico come quello degli oggetti macroscopici. Lo spin di un elettrone può essere orientato verso l'alto o verso il basso, corrispondente agli stati binari 0 e 1 utilizzati nei computer classici. Tuttavia, grazie ai principi della meccanica quantistica, lo spin può anche trovarsi in una sovrapposizione quantistica, il che significa che può essere simultaneamente in entrambi gli stati, 0 e 1, fino a quando non viene misurato. Questa capacità di trovarsi in una sovrapposizione rende il qubit molto più potente rispetto al bit classico, permettendo di eseguire calcoli complessi in parallelo.

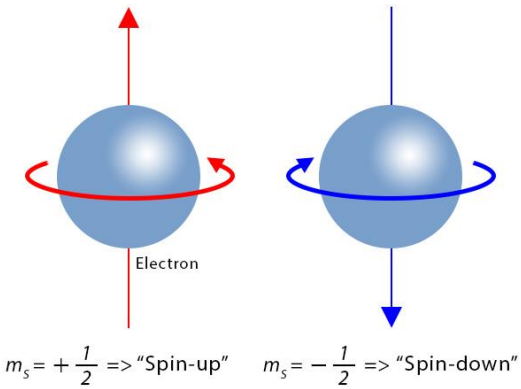

Figura 15: Gli spin dell'elettrone, dove m_s indica l'orientamento dello spin dell'elettrone

Nei sistemi che utilizzano qubit basati su spin, come nei semiconduttori o nei punti quantici, il controllo dello spin avviene tramite l'applicazione di campi magnetici o impulsi di microonde, che permettono di manipolare lo stato quantistico. Una volta che lo spin viene manipolato, può essere misurato per ottenere informazioni sullo stato del qubit.

I qubit possono essere realizzati utilizzando diverse tecnologie e approcci fisici. Tra le metodologie più comuni ci sono i circuiti superconduttori, gli ioni intrappolati, i punti quantici e i fotoni. I circuiti superconduttori, ad esempio, sfruttano la fisica dei materiali a basse temperature per creare qubit estremamente stabili, oppure si sfruttano gli ioni intrappolati, i quali vengono manipolati all'interno campi elettromagnetici per mantenere la loro stabilità e ridurre la possibilità di decoerenza. Ogni tecnologia ha i suoi punti di forza e debolezza, e la scelta di una particolare implementazione dipende in gran parte dall'applicazione specifica e dalla sfida tecnica che si intende affrontare. [40]

Una delle proprietà più importanti dei qubit è la loro capacità di essere "entangled", o intrecciati, con altri qubit, il cui fenomeno consente ai qubit di condividere informazioni in modo istantaneo anche a grandi distanze, con potenziali applicazioni che spaziano dalla crittografia quantistica alle simulazioni fisiche avanzate, come la riproduzione digitale di una proteina. Sebbene i qubit portino enormi vantaggi, il mantenimento della stabilità è uno degli

ostacoli principali nella ricerca. Infatti, i qubit sono estremamente sensibili all'ambiente esterno, e anche piccole interferenze possono causarne la decoerenza, rendendoli inefficaci, causando errori nei calcoli quantistici.

Le sfide tecniche legate alla stabilizzazione dei qubit includono la necessità di mantenere temperature estremamente basse, spesso vicine allo zero assoluto, e la gestione delle interferenze esterne, che può causare la perdita di coerenza. Negli ultimi anni i progressi nella correzione degli errori quantistici stanno migliorando la stabilità dei sistemi quantistici, permettendo di avvicinarsi sempre più alla realizzazione di computer quantistici pienamente funzionanti.

I qubit rappresentano dunque il fulcro del calcolo quantistico e delle sue promesse rivoluzionarie, che grazie alle loro capacità uniche, i computer quantistici potrebbero presto affrontare problemi di complessità inaccessibile per i computer classici, aprendo nuove possibilità in settori come la chimica computazionale, la crittografia e l'intelligenza artificiale. [41]

2.3. Modelli di Computer Quantistici

Nel campo del calcolo quantistico, lo sviluppo e l'applicazione di diversi modelli di computer quantistici rappresentano un'area di ricerca in rapido progresso. Si distinguono per i materiali utilizzati e per le tecnologie impiegate per realizzare i qubit e manipolarli, cercando di risolvere i problemi di stabilità, scalabilità e correzione degli errori. Le soluzioni ingegneristiche variano significativamente, dando luogo a differenti architetture con capacità specifiche e vantaggi competitivi.

Figura 14: Computer quantistico di IBM [42]

2.3.1. Tecnologie Basate sul Silicio

Un primo approccio per la realizzazione di computer quantistici è quello di sfruttare un materiale il cui settore è ben sviluppato: il Silicio. Questa scelta rappresenta una continuazione del paradigma tradizionale della microelettronica, andando ad aggirare la Legge di Moore. Questi tipi di computer sfruttano i punti quantici introdotti nel silicio per immagazzinare e manipolare qubit, permettendo così una potenziale scalabilità. Attraverso questa tecnologia, si mira a creare qubit di spin sul silicio a livello atomico, sfruttando la coerenza delle interazioni di spin per mantenere l'informazione quantistica stabile. L'utilizzo del Silicio permette una maggiore compatibilità con le attuali strutture di fabbricazione, consentendo la creazione di chip quantistici su larga scala, riducendo i costi di produzione e aumentando la densità dei qubit. [43]

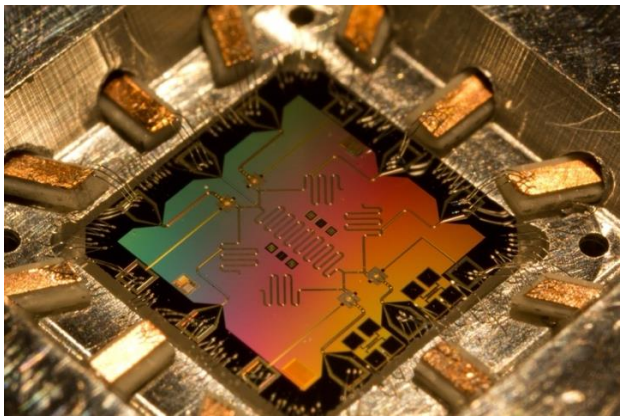

Figura 15: Processore quantistico basato sul Silicio [44]

2.3.2. Tecnologia Ionica

La tecnologia basata sugli ioni intrappolati negli ultimi anni ha ottenuto grandi risultati e risulta essere molto promettente. Tramite dei campi elettromagnetici, le particelle atomiche caricate elettricamente, gli ioni, vengono confinate e sospese nello spazio. Ogni qubit viene immagazzinato negli stati elettronici stabili di ciascun ione, e successivamente vengono accoppiati e manipolati tramite appositi laser. Questa tecnologia non è particolarmente soggetta ai disturbi esterni in quanti gli ioni sono particolarmente stabili e si riesce a manipolare i qubit in maniera "semplice" rispetto ad altri modelli di computer quantistici. I tempi di decoerenza sono particolarmente lunghi, rendendo questo approccio promettente per la realizzazione di computer scalabili, specialmente nel contesto della ricerca accademica e dei primi prototipi di dispositivi quantistici. Tuttavia, la gestione dei laser

richiesti è difficile e intrappolare in modo corretto gli ioni è notevolmente complesso, soprattutto se sono presenti in grandi quantità.
[45]

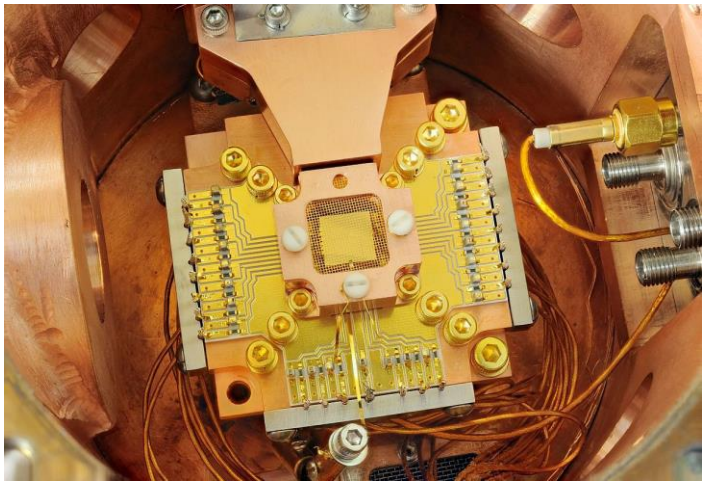

Figura 16: Computer quantistico a ioni intrappolati [46]

2.3.3. Computer Quantistici Fotonici

I fotoni, particelle di luce, non sono soggetti a interazioni deboli con l'ambiente esterno, ciò li rende particolarmente resistenti alla decoerenza. Questo tipo di computer sfrutta i fotoni come qubit, i quali possono essere rappresentati da stati sovrapposti all'interno di impulsi luminosi. In particolare, gli stati compressi (squeeze states) vengono utilizzati per ridurre l'incertezza in alcune variabili del sistema, migliorando la precisione delle operazioni quantistiche. I fotoni vengono manipolati tramite porte ottiche e componenti costruiti con tecniche di progettazione al silicio, costituendo un grande potenziale di scalabilità fino a milioni di qubit, offrendo così un modo di sviluppare computer quantistici su larga scala senza i problemi tipici della decoerenza che affliggono gli altri modelli. Tuttavia, il calcolo fotonico è complesso e richiede l'implementazione di componenti ottiche sofisticate, con un controllo preciso dei fotoni, ponendo sfide significative per l'applicazione su vasta scala.
[47]

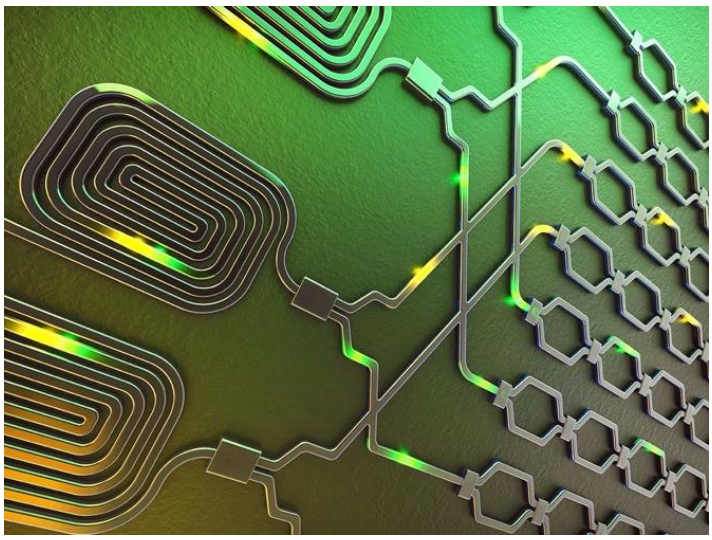

Figura 17: Rappresentazione di un computer quantistico fotonico [48]

2.3.4. Utilizzo di Superconduttori

Un'altra tecnologia ampiamente esplorata è quella basata dui superconduttori, dove i qubit vengono creati tramite fotoni o stati esotici della materia intrappolati in campi magnetici. I materiali superconduttori a temperature estremamente basse permettono il passaggio di corrente senza alcuna resistenza, offrendo così un ambiente perfetto per l'esecuzione di operazioni quantistiche con tempi di decoerenza ridotti. I circuiti quantistici che sfruttano i superconduttori in ambienti criogenici operano in un ambiente in cui le proprietà fisiche del sistema cambiano e permettono calcoli notevolmente rapidi. Questo tipo di computer viene largamente utilizzato per la creazione di dispositivi di calcolo quantistici, e sono alla base dell'architettura di molte macchine sviluppate da grandi aziende come Google (Sycamore) e IBM. La difficoltà di questa architettura risiede nel mantenere le temperature dei superconduttori estremamente basse, aumentandone la complessità e i costi. [49]

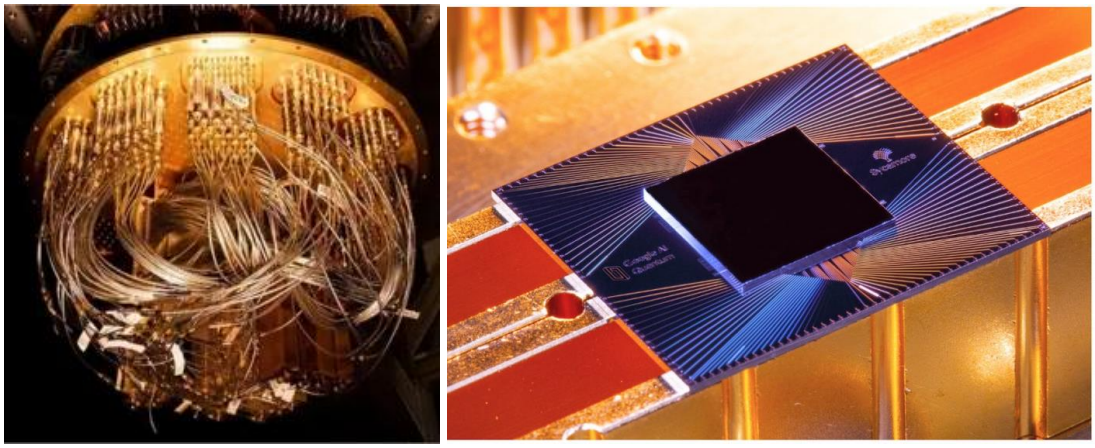

Figura 18: Sycamore e il suo processore creati da Google [50]

2.4. Algoritmi Quantistici e Applicazioni

Nel corso degli ultimi decenni assieme alla creazione dei computer quantistici si sono visti algoritmi che potessero essere sfruttati a pieno da essi. Questi calcoli sono adattati proprio per queste macchine innovative e non sono compatibili con i processori tradizionali.

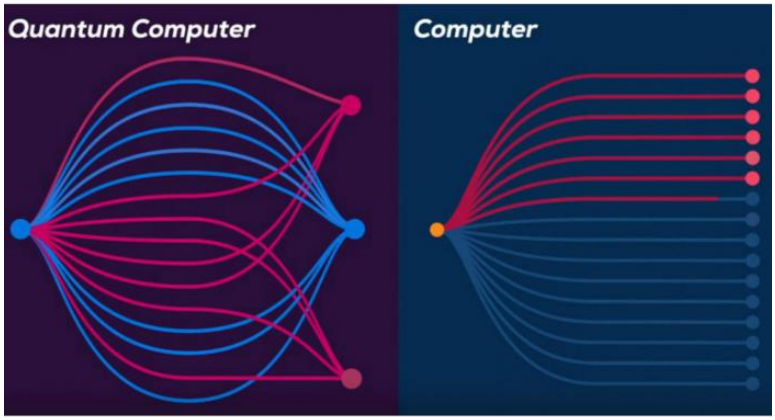

Figura 19: Rappresentazione della differenza tra algoritmi quantistici e tradizionali [51]

2.4.1. Algoritmo di Shor

Sviluppato da Peter Shor nel 1994, è uno degli algoritmi più noti nell'ambito del calcolo quantistico. Esso risolve il problema della fattorizzazione di numeri interni molto grandi in tempi polinomiali, un compito che i classici computer richiederebbero un tempo esponenziale. Si stima che, anche utilizzando le tecnologie di calcolo classico più avanzate, il tempo necessario per completare la fattorizzazione che comprometterebbe lo schema crittografico RSA a 2048 bit si misurerebbe in trilioni di anni. Se invece si utilizzasse un computer quantistico con sufficienti risorse in termini di memoria e capacità di calcolo, l'algoritmo di Shor potrebbe effettuare la stessa operazione in poche ore. Per rendere possibile ciò, l'algoritmo di Shor sfrutta il parallelismo quantistico e la trasformata quantistica di Fourier, utilizzabili solamente nel calcolo quantistico. Questo algoritmo può essere si utilizzato in maniera negativa per superare facilmente la crittografia, ma d'altra parte può essere sfruttato per migliorare l'analisi dei dati crittografati nel contesto della sicurezza bancaria e delle transizioni finanziarie.

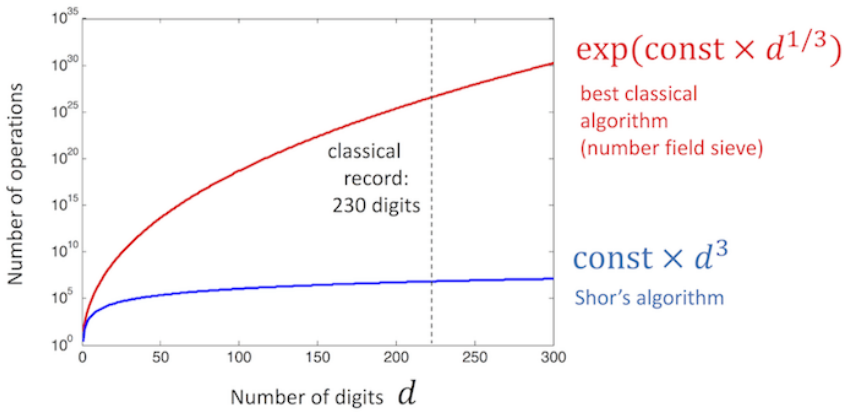

Figura 20: Stima del numero di operazioni in base al numero di cifre, tramite l'algoritmo di Shor e tramite il migliore algoritmo tradizionale [52]

2.4.2. Algoritmo di Grover

Altro algoritmo molto importante nella computazione quantistica è quello ideato da Lov Grover nel 1996, con lo scopo di migliorare l'efficienza della ricerca in database non strutturati. L'algoritmo di Grover, sfruttando l'interferenza quantistica, consente la ricerca di un elemento in un database di dimensione n, con complessità temporale di $O(\sqrt{n})$; a differenza degli algoritmi utilizzati nei computer classici che eseguono la ricerca in tempi $O(n)$. Le sue applicazioni sono molteplici, tra cui la ricerca di soluzioni di problemi complessi di ottimizzazione e miglioramento delle performance di intelligenza artificiale, dove le operazioni di ricerca e ordinamento dei dati sono alla base. [53]

2.4.3. Simulazioni quantistiche

Probabilmente l'area in cui i computer quantistici dimostrano il massimo della loro potenza è quella della simulazione di sistemi quantistici complessi, come molecole e materiali. I computer classici sono limitati dalla loro capacità di simulare accuratamente sistemi quantistici, i computer quantistici sfruttano direttamente i principi della meccanica quantistica per modellare queste interazioni. Le simulazioni quantistiche sono particolarmente utili in ambiti come la chimica computazionale, la creazione di nuovi farmaci, e la progettazione di materiali innovativi con proprietà specifiche. Un esempio pratico è la possibilità di accelerare la scoperta di nuovi catalizzatori o composti chimici per la produzione di energia pulita. Oppure l'uso dei computer quantistici per studiare fenomeni fisici complessi come la superconduttività e l'energia solare. Grazie al miglioramento di queste tecnologie si prevede che si possa rivoluzionare il modo in cui si affrontano problemi di chimica, fisica e biologia molecolare. [54]

2.5. Sfide attuali del Quantum computing

Sebbene i computer quantistici siano molto promettenti ed è probabile che porteranno una rivoluzione nel mondo dell'informatica, essi presentano diversi problemi molto complessi da superare, che ne rallentano lo sviluppo e ne posticipano la vera e propria rivoluzione.

2.5.1. Scalabilità

Uno degli ostacoli maggiori è quello della scalabilità dei sistemi quantistici, i quali possiedono tecnologie molto complesse come gli ioni intrappolati o i circuiti superconduttori, ma queste architetture permettono di operare con un numero limitati di qubit. Per realizzare un computer quantistico su vasta scala sono necessari un numero di qubit significativamente maggiore rispetto alle quantità che vengono utilizzate oggi. Di conseguenza però, con l'aggiunta di nuovi quantum bit, la gestione e manipolazione di essi, aumenta notevolmente la complessità e il rischio di errori derivanti dalla decoerenza e dal rumore. [55]

2.5.2. Mantenimento della Coerenza quantistica

La capacità di un sistema quantistico di mantenere stati sovrapposti, chiamata coerenza quantistica, è estremamente complessa e fragile. Piccole interazioni con l'ambiente esterno posso causare decoerenza, distruggendo così le proprietà quantistiche del sistema e portando a errori nello sviluppo dei calcoli. L'obiettivo è mantenere la coerenza per il maggior tempo possibile, in modo da poter eseguire i calcoli quantistici in un ambiente "sicuro". Sono diverse le tecniche per la correzione degli errori che si stanno sviluppando, ma ora come ora non è possibile posticipare significativamente la decoerenza in modo da poter sviluppare dei computer quantistici su larga scala. [56]

2.5.3. Requisiti energetici

Un altro aspetto critico riguarda i requisiti energetici. Infatti, i computer quantistici operano in condizioni estreme, dove le temperature raggiungono quasi lo zero assoluto per mantenere i qubit stabili. Per sostenere queste condizioni è richiesto un enorme dispendio di energia che addirittura supera la quantità di energia richiesta per i calcoli quantistici stessi, contrariamente a quanto avviene nei computer classici. Pertanto, un futuro sostenibile

per i computer quantistici richiede miglioramenti sia nell'efficienza energetica che nella progettazione di sistemi termici avanzati. [56]

Conclusioni

Nel corso della storia, lo sviluppo dei processori in silicio ha rappresentato un elemento fondamentale nella crescita del mondo dell'informatica e non solo. Fin dalla sua introduzione, il silicio è stato il materiale chiave per la creazione di semiconduttori, permettendo la miniaturizzazione dei transistor e la continua evoluzione della Legge di Moore, che ha previsto il costante raddoppio della densità dei transistor ogni 18-24 mesi. Questa progressione ha portato a computer sempre più potenti e accessibili, trasformando intere industrie e realtà. Tuttavia, con il progressivo raggiungimento dei limiti fisici del silicio, i tradizionali processori si avvicinano a un punto in cui l'ulteriore miniaturizzazione diventa sempre più complessa e dispendiosa. Questo ha spinto la ricerca verso nuove tecnologie alternative e complementari, tra cui il calcolo quantistico.

Basati sulla meccanica quantistica, i computer quantistici rappresentano una svolta rivoluzionaria per il settore dell'informatica e non solo. A differenza dei processori tradizionali che si basano su bit binari (0 e 1), i computer quantistici sfruttano i qubit, i quali possiedono la capacità di sovrapposizione degli stati e di "intrecciarsi" tra loro tramite l'entanglement. Ciò permette di affrontare problemi inaccessibili tramite il calcolo tradizionale, consentendo di svolgere per esempio simulazioni di molecole complesse o la risoluzione di problemi di ottimizzazione a una velocità significativamente maggiore.

Sebbene gli sviluppi promettenti, i computer quantistici sono ancora nelle fasi iniziali e affrontano ancora innumerevoli sfide, per esempio: la stabilità dei qubit e la correzione degli errori. I sistemi quantistici risultano essere ancora troppo fragili e sensibili all'ambiente esterno impedendo di conseguenza un utilizzo corretto e specifico per determinati settori. Tuttavia, le ricerche per la creazione di nuove tecnologie di correzione degli errori e il miglioramento della stabilità dei qubit sono l'obiettivo principale nel campo.

Nonostante le difficoltà, le prospettive future del quantum computing sono promettenti. La continua innovazione tecnologica potrebbe portare a computer quantistici utilizzabili in ambiti specifici, mentre i computer classici continueranno a dominare nelle applicazioni quotidiane, creando una collaborazione tra le due diverse architetture.

In conclusione, i processori in silicio hanno segnato la storia dell'informatica e dell'intero pianeta, continueranno ad evolversi sebbene i limiti fisici imposti dal materiale stiano spingendo la ricerca di nuove frontiere. I computer quantistici costituiscono una di queste nuove frontiere, e con il loro sviluppo si prevede una sinergia tra i due approcci, che potrebbe unire i punti di forza di ciascuno per risolvere sfide comuni.

Bibliografia

[1] J. K. Pushkar Ranade, «Bits and Bytes,» 16 07 2023. [Online]. Available: https://semiconductor.substack.com/p/the-relentless-pursuit-of-moores.

[2] «Apple svela M1 Ultra, il chip più potente al mondo per un personal computer,» 2022. [Online]. Available: https://www.apple.com/it/newsroom/2022/03/apple-unveils-m1-ultra-the-worlds-most-powerful-chip-for-a-personal-computer/.

[3] A. dhara, «Geeks ULTD,» 13 04 2022. [Online]. Available: https://www.geeksultd.com/2022/04/moores-law-remains-alive-thanks-to-apples-monster-m1-ultra-chip/.

[4] S. Cass, «Chip Hall of Fame: Intel 4004 Microprocessor,» 02 07 2018. [Online]. Available: https://spectrum.ieee.org/chip-hall-of-fame-intel-4004-microprocessor#:~:text=The%20Intel%204004%20was%20the,CPU%20on%20a%20single%20chip.

[5] [Online]. Available: https://it.wikipedia.org/wiki/Intel_4004#/media/File:Intel_4004.jpg.

[6] [Online]. Available: https://it.wikipedia.org/wiki/Intel_8080#/media/File:Intel_C8080A_9064_33001_N8384_top.jpg.

[7] [Online]. Available: https://deramp.com/downloads/intel/8080%20Data%20Sheet.pdf.

[8] [Online]. Available: https://it.wikipedia.org/wiki/Altair_8800#/media/File:Altair_8800_computer.jpg.

[9] [Online]. Available: https://it.wikipedia.org/wiki/IMSAI_8080#/media/File:IMSAI_8080-IMG_1477.jpg.

[10] «History Tools,» 25 03 2024. [Online]. Available: https://www.historytools.org/companies/intel-history.

[11] «32-bit application,» 11 12 1995. [Online]. Available: https://foldoc.org/32-bit+application.

[12] «32-bit computing,» [Online]. Available: https://www.pcmag.com/encyclopedia/term/32-bit-computing#:~:text=Although%2032%2Dbit%20CPUs%20were,bit%20applications%20(see%20386)..

[13] J. Prosise, «16 or 32 Bits: Should It Matter to You?,» *PC Magazine,* pp. 321-322, 07 11 1995.

[14] G. Bucci, «Questo documento è una appendice al volume Calcolatori Elettronici - Architettura e Organizzazione IV edizione,» 31 03 2017. [Online]. Available: http://cvg.dsi.unifi.it/colombo_now/calc/Bucci_2017/AppC.pdf.

[15] «Microelettronica,» [Online]. Available: https://www.treccani.it/enciclopedia/microelettronica/.

[16] S. Thornton, «Multicore processors terminology,» 3 3 2017. [Online]. Available: https://www.microcontrollertips.com/terminology-multicore-processors/.

[17] S. J. Bigelow, «multicore processor,» 3 2022. [Online]. Available: https://www.techtarget.com/searchdatacenter/definition/multi-core-processor.

[18] K. Hinum, «Apple MacBook Air 2020 M1 Entry Review: Apple M1 CPU humbles Intel and AMD,» 12 05 2020. [Online]. Available: https://www.notebookcheck.net/Apple-MacBook-Air-2020-M1-Entry-Review-Apple-M1-CPU-humbles-Intel-and-AMD.508057.0.html.

[19] F. L. Trofa, «NPU (Neural Processing Unit): cosa sono i processori per l'intelligenza artificiale degli AI PC,» 15 07 2024. [Online]. Available: https://www.sergentelorusso.it/npu-neural-processing-unit-cosa-sono/.

[20] «Deploying Transformers on the Apple Neural Engine,» 06 2022. [Online]. Available: https://machinelearning.apple.com/research/neural-engine-transformers.

[21] Apple, «Newsroom,» 10 11 2020. [Online]. Available: https://www.apple.com/it/newsroom/2020/11/apple-unleashes-m1/.

[22] K. Freund, «Google's TPU Chip Creates More Questions Than Answers,» 26 05 2016. [Online]. Available: https://www.forbes.com/sites/moorinsights/2016/05/26/googles-tpu-chip-creates-more-questions-than-answers/.

[23] A. Troise, «CPU, GPU, and NPU: Understanding Key Differences and Their Roles in Artificial Intelligence,» 18 06 2024. [Online]. Available: https://levysoft.medium.com/cpu-gpu-and-npu-understanding-key-differences-and-their-roles-in-artificial-intelligence-2913a24d0747.

[24] T. Duque, «New Silicon Nanowires Can Really Take the Heat,» 17 05 2022. [Online]. Available: https://newscenter.lbl.gov/2022/05/17/silicon-nanowires-take-the-heat/.

[25] J. Dascalu, «As node sizes shrink, manufacturing challenges grow,» 21 08 2024. [Online]. Available: https://electronics360.globalspec.com/article/21403/as-node-sizes-shrink-manufacturing-challenges-grow.

[26] J. Haller, «An introduction to quantum computing architecture,» 16 02 2021. [Online]. Available: https://www.redhat.com/architect/quantum-computing.

[27] «Qubit vs Bit: The Key Differences Explained,» 04 03 2024. [Online]. Available: https://quantumexplainer.com/qubit-vs-bit-the-key-differences-explained/.

[28] A. Miller, «Qubits vs Bits: How Quantum and Classical Computing Differ,» 15 03 2024. [Online]. Available: https://rehack.com/tech-explained/qubits-vs-bits/.

[29] «Quantum computing,» 23 08 2023. [Online]. Available: https://www.explainthatstuff.com/quantum-computing.html.

[30] [Online]. Available: https://its.unc.edu/wp-content/uploads/sites/337/2021/06/Introduction_to_Quantum_Computers.pdf.

[31] E. Rieffel e W. Polak, «An Introduction to Quantum Computing for Non-Physicists,» [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/367701.367709.

[32] «Superposition and entanglement,» [Online]. Available: https://www.quantum-inspire.com/kbase/superposition-and-entanglement/.

[33] V. Novara, «Meccanica quantistica: il principio di sovrapposizione,» 21 09 2021. [Online]. Available: https://www.passioneastronomia.it/meccanica-quantistica-il-principio-di-sovrapposizione/.

[34] D. Bonacorsi. [Online]. Available: https://sanomaitalia.it/aree-disciplinari/scienze/quantum-computing.

[35] A. Parlangeli, «Avete capito cos'è l'entanglement quantistico che è valso il Nobel per la fisica? E a "che serve"?,» 04 10 2022. [Online]. Available: https://www.focus.it/scienza/scienze/che-cos-entanglement-quantistico-nobel-fisica-applicazioni.

[36] V. Vedral, «Quantum entanglement,» *Nature Physics,* pp. 256-259, 2014.

[37] «Roots of quantum computing supremacy: superposition, entanglement, or complementarity?,» 13 04 2021. [Online]. Available: https://link.springer.com/article/10.1140/epjs/s11734-021-00061-9.

[38] L. N. N. J. C. Benoit Seron, «Boson bunching is not maximized by indistinguishable particles,» 15 06 2023. [Online]. Available: https://www.nature.com/articles/s41566-023-01213-0.

[39] «Cos'è il calcolo quantistico?,» [Online]. Available: https://azure.microsoft.com/it-it/resources/cloud-computing-dictionary/what-is-quantum-computing.

[40] I. S. Josh Schneider, «Cos'è un qubit?,» 28 02 2024. [Online]. Available: https://www.ibm.com/it-it/topics/qubit.

[41] IBM, «Cos'è il quantum computing?,» [Online]. Available: https://www.ibm.com/it-it/topics/quantum-computing.

[42] S. Scalia, «Computer quantistici – Potenzialità e rischi,» 03 11 2023. [Online]. Available: https://www.futurajob.it/computer-quantistici-potenzialita-e-rischi/.

[43] F. AHMAD, «Silicon-based Quantum Computing,» 20 07 2023. [Online]. Available: https://medium.com/quantum-engineering/silicon-based-quantum-computing-af136a56e921.

[44] H. Despa, «Quantum Computing Is Complete As Researchers Build the First Two-Qubit Logic in Silicon,» 09 09 2015. [Online]. Available: https://news.softpedia.com/news/quantum-computing-is-complete-as-researchers-build-the-first-two-qubit-logic-in-silicon-494156.shtml.

[45] «Atoms make better quantum computers,» [Online]. Available: https://ionq.com/technology.

[46] Y. Colombe, «Quantum Computing; Ion Trapping,» 23 02 2011. [Online]. Available: https://www.nist.gov/image/quantumcomputingiontrappingjpg.

[47] G. M. Jacquiline Romero, «Photonic Quantum Computing,» 04 04 2024. [Online]. Available: https://arxiv.org/html/2404.03367v1.

[48] N. Savage, «Building Quantum Computers With Photons,» 05 09 2018. [Online]. Available: https://spectrum.ieee.org/building-quantum-computers-with-photons.

[49] A. Ballon, «Quantum computing with superconducting qubit,» 22 03 2022. [Online]. Available: https://pennylane.ai/qml/demos/tutorial_sc_qubits/.

[50] M. Schneider, «Computer Science: Google's "Sycamore" Chip—First Proof of Concept for "Quantum Supremacy"?,» 03 11 2019. [Online]. Available: https://www.linkedin.com/pulse/computer-science-googles-sycamore-chipfirst-proof-michael-schneider/.

[51] Kurzgesagt, «Quantum Computers Explained – Limits of Human Technology,» 08 12 2015. [Online]. Available: https://futuristech.info/posts/video-quantum-computers-simplified-sort-of-in-a-nutshell.

[52] E. Frumento, «Quantum Key Distribution: cos'è e perché è utile a rendere inattaccabili i sistemi di cifratura,» 23 06 2022. [Online]. Available: https://www.cybersecurity360.it/soluzioni-aziendali/quantum-key-distribution-cose-e-perche-e-utile-a-rendere-inattaccabili-i-sistemi-di-cifratura/.

[53] «Quali sono i componenti chiave dell'algoritmo di Grover e come contribuiscono al processo di ricerca?,» 06 08 2023. [Online]. Available: https://it.eitca.org/quantum-information/eitc-qi-qif-quantum-information-

fundamentals/grovers-quantum-search-algorithm/needle-in-a-haystack/examination-review-needle-in-a-haystack/what-are-the-key-components-of-grovers-algorithm-and-how-do-they-contribute.

[54] S. R. C. D. J. Tomi H Johnson, «What is a quantum simulator?,» 23 07 2014. [Online]. Available: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt10.

[55] A. K. I. S. Yuri Alexeev, «Challenges and Opportunities of Scaling Up Quantum Computation and Circuits,» 01 05 2024. [Online]. Available: https://www.siam.org/publications/siam-news/articles/challenges-and-opportunities-of-scaling-up-quantum-computation-and-circuits/.

[56] C. H. G. M. E. B. J. D. S. S. N. R. G. Michael James Martin, «Energy use in quantum data centers: Scaling the impact of computer architecture, qubit performance, size, and thermal parameters,» [Online]. Available: https://arxiv.org/pdf/2103.16726.

Immagini