

OVERVIEW OF QUANTUM COMPUTERS - THE PROBLEMS POSED

Do Thi Bac*, Phonekeopaserth Soulivong, Khit Bounsaveng

TNU – University of Information and Communication Technology

ARTICLE INFO		ABSTRACT
Received:	13/3/2023	Quantum computing is a field that is still very new and does not have a commonly used product yet. This paper provides an overview of quantum computing and evaluates research from the birth of quantum computing to the present day. The analysis covers various aspects, such as the birth of quantum computing, its developmental progress, and questions related to prospects, visions, challenges, and opportunities. It also explains the power of quantum computing, which is based on the principles of quantum mechanics such as quantum superposition, quantum entanglement, and the uncertainty principle. The methodology used in this study involves analyzing, synthesizing, and comparing information to draw valuable conclusions and comments. This article is useful for those who are starting to study quantum computers, as it provides an overview of the field and offers guidance for research work. Additionally, it can aid regulators, governments, and other organizations in making decisions and policies related to quantum computing platforms.
Revised:	15/5/2023	
Published:	15/5/2023	
KEYWORDS		
Quantum computer		
Hadamard gate		
Shor's algorithm		
Qubit		
Superposition		

TOÀN CẢNH VỀ MÁY TÍNH LƯỢNG TỬ - NHỮNG VẤN ĐỀ ĐẶT RA

Đỗ Thị Bắc*, Phonekeopaserth Soulivong, Khit Bounsaveng

Trường Đại học Công nghệ Thông tin và Truyền thông - ĐH Thái Nguyên

THÔNG TIN BÀI BÁO		TÓM TẮT
Ngày nhận bài:	13/3/2023	Máy tính lượng tử - một lĩnh vực còn rất mới và là loại máy tính chưa được sử dụng phổ biến. Bài báo này trình bày tổng quan về máy tính lượng tử và đánh giá các nghiên cứu từ khi ra đời cho đến nay bao gồm: sự ra đời, tiến trình phát triển đến những vấn đề đặt ra về triển vọng, tầm nhìn, thách thức và cơ hội. Đồng thời cũng giải thích sức mạnh của máy tính lượng tử thông qua công nghệ tính toán lượng tử dựa trên các nguyên lý của cơ học lượng tử, chẳng hạn như siêu đặc tính lượng tử, sự liên kết lượng tử, hoặc định lý không thể sao chép. Phương pháp được sử dụng trong nghiên cứu này phân tích, tổng hợp và so sánh thông tin để đánh giá và đưa ra những kết luận và nhận xét có giá trị. Bài báo hữu ích cho những người mới bắt đầu nghiên cứu về máy tính lượng tử, giúp họ có được cái nhìn tổng quan về lĩnh vực máy tính lượng tử và định hướng cho công việc nghiên cứu của họ. Nó cũng có thể giúp các nhà quản lý, chính phủ và các tổ chức khác trong việc đưa ra các quyết định và chính sách liên quan đến nền tảng máy tính lượng tử.
Ngày hoàn thiện:	15/5/2023	
Ngày đăng:	15/5/2023	
TỪ KHÓA		
Máy tính lượng tử		
Cổng Hadamard		
Thuật toán Shor		
Qubit		
Chồng chất		

DOI: <https://doi.org/10.34238/tnu-jst.7523>

* Corresponding author. Email: dtbac@ictu.edu.vn

1. Giới thiệu

Máy tính lượng tử (MTLT) là một loại máy tính mới, được thiết kế để thực hiện các tính toán sử dụng nguyên tử và phân tử [1] – [7], thay vì sử dụng các mạch điện tử như máy tính truyền thống (MTTT). Điều này cho phép MTLT xử lý thông tin với tốc độ rất nhanh và độ chính xác cao hơn so với máy tính cổ điển [8] – [15].

Một sự khác biệt lớn giữa MTLT và MTTT là cách thực hiện tính toán. MTLT sử dụng các qubit (đơn vị thông tin lượng tử) để thực hiện tính toán, trong khi MTTT sử dụng các bit nhị phân thông thường [16] – [22]. Các qubit có thể tồn tại ở nhiều trạng thái khác nhau cùng một lúc, cho phép MTLT thực hiện nhiều tính toán đồng thời, trong khi MTTT chỉ có thể thực hiện một tính toán tại một thời điểm.

Một số ứng dụng tiềm năng của MTLT bao gồm việc giải quyết các bài toán phức tạp trong lĩnh vực vật lý, hóa học, sinh học, tài chính và thương mại điện tử [1] – [7], [22] – [30]. Ví dụ, MTLT có thể được sử dụng để thiết kế các vật liệu mới với tính chất đặc biệt [6], giải quyết các bài toán về tối ưu hóa đầu tư tài chính [4], [25], [27], [29], hoặc giúp tạo ra các sản phẩm mới trong thương mại điện tử [1], [27]. MTLT cũng có thể được sử dụng để mô phỏng các hiện tượng vật lý phức tạp [1], [2], [16], [28], giúp các nhà khoa học hiểu rõ hơn về vũ trụ và các hiện tượng vật lý khác.

Tuy nhiên, việc phát triển MTLT vẫn còn rất mới và đang gặp nhiều thách thức, bao gồm việc xử lý các lỗi lượng tử [4], [20], tăng cường độ tin cậy và độ chính xác của MTLT [31] – [35], và tạo ra các thiết bị lượng tử phù hợp với các ứng dụng thực tế [4], [5], [35].

Bài báo này cung cấp một cái nhìn tổng quan về tình hình phát triển của công nghệ MTLT trên thế giới, từ khi xuất hiện cho đến hiện tại. Bài báo cũng giải thích về khái niệm MTLT, sự khác biệt giữa MTLT và máy tính cổ điển, những tiềm năng và thách thức của công nghệ này.

Đồng thời, bài báo cũng đề cập đến các dự án nghiên cứu hiện tại và tương lai về MTLT, các phương pháp mới trong việc thiết kế, phát triển và sử dụng MTLT, cũng như những tiến bộ đáng chú ý trong lĩnh vực này nhằm giúp độc giả hiểu rõ hơn về công nghệ MTLT và ứng dụng của nó trong các lĩnh vực khác nhau.

2. Phương pháp nghiên cứu

MTLT là một lĩnh vực khoa học còn rất mới trên thế giới và ở Việt Nam. Hiện tại MTLT chưa được sử dụng phổ biến mới chỉ được nghiên cứu và sử dụng trong các phòng thí nghiệm của các tập đoàn lớn trên thế giới. Vì vậy trong bài báo tổng quan này chúng tôi sử dụng các phương pháp nghiên cứu chủ yếu sau:

Phân tích tài liệu: Phương pháp này bao gồm đánh giá các tài liệu trước đây đã được xuất bản về chủ đề MTLT đang đề cập. Việc này giúp đánh giá tình hình nghiên cứu hiện tại, những câu hỏi còn đang mơ hồ và những vấn đề chưa được giải quyết trong lĩnh vực này.

Phân tích nội dung: Phương pháp này giúp đánh giá các tài liệu trước đây để phát hiện ra các vấn đề, xu hướng chính trong lĩnh vực MTLT.

Phân tích hệ thống: đây là bài báo tổng quan đang đề cập đến một lĩnh vực phức tạp, phương pháp phân tích hệ thống được sử dụng để đưa ra cái nhìn toàn diện về các mối quan hệ giữa các yếu tố khác nhau trong lĩnh vực đó.

3. Kết quả nghiên cứu và bài luận

3.1. Lịch sử và tiến trình phát triển của MTLT

3.1.1. Sự ra đời của máy tính lượng tử

MTLT là một trong những công nghệ tiên tiến nhất của thế kỷ 21. Tuy nhiên, ý tưởng về MTLT đã xuất hiện từ rất sớm, vào những năm đầu của thế kỷ 20. Những năm đầu 1900, nhà toán học người Đức Max Planck đưa ra định luật bức xạ, trong đó ông giới thiệu khái niệm "hạt"

của ánh sáng [1], [4], [5]. Điều này đánh dấu sự khởi đầu của lý thuyết về cơ học lượng tử. Sau đó, các nhà khoa học khác như Albert Einstein, Niels Bohr, Werner Heisenberg và Erwin Schrödinger đã phát triển các khái niệm và công thức toán học để mô tả cơ học lượng tử [21], [22], [24]. Trong những năm 1980, Richard Feynman đã đề xuất ý tưởng về MTLT trong bài phát biểu tại “Hội nghị Vật lý Công nghệ và Giới hạn của nó” tại MIT [1], [4]. Tuy nhiên, đến tận năm 1994, Peter Shor đã công bố một giải thuật giải mã số nguyên tố bằng MTLT [4], [28], chứng tỏ rằng MTLT có thể giải quyết các bài toán phức tạp mà MTTT không thể.

Kể từ đó, nhiều nhà khoa học và các công ty công nghệ hàng đầu trên thế giới đã bắt đầu đầu tư nghiên cứu và phát triển MTLT. Trong vài thập kỷ qua, MTLT đã được phát triển nhanh chóng và trở thành một trong những công nghệ tiên tiến nhất hiện nay, các nhà nghiên cứu đang tiếp tục nghiên cứu và phát triển các thiết bị, công nghệ liên quan đến MTLT, với mục tiêu tạo ra các MTLT hoàn hảo hơn, có khả năng giải quyết các bài toán phức tạp hơn nữa.

3.1.2. Tiến trình phát triển của MTLT

Trong quá trình phát triển MTLT, đã có nhiều thành tựu đáng chú ý đã đạt được. Dưới đây là một số ví dụ:

- ✓ Thiết bị đầu tiên sử dụng nguyên lý lượng tử: MTLT đầu tiên được giới thiệu vào năm 1982 bởi Richard Feynman và Paul Benioff [1], [5], [6]. Thiết bị này sử dụng nguyên lý của lượng tử để thực hiện các phép tính.

- ✓ Cổng cơ bản của MTLT: Cổng Hadamard, được giới thiệu vào năm 1995 bởi Peter Shor và Leonard Grover [1], [4], là một cổng cơ bản của MTLT. Nó cho phép chuyển đổi trạng thái của một qubit từ trạng thái cơ bản sang trạng thái siêu dẫn.

- ✓ Thuật toán Shor: Thuật toán Shor, được giới thiệu vào năm 1994 bởi Peter Shor, là một thuật toán quan trọng trong MTLT. Nó có thể giải quyết bài toán phân tích số nguyên tố nhanh hơn các thuật toán truyền thống [1].

- ✓ Thiết bị lưu trữ thông tin lượng tử: Thiết bị lưu trữ thông tin lượng tử (quantum memory) cho phép lưu trữ thông tin ở dạng lượng tử trong thời gian dài hơn [3], [8]. Điều này rất quan trọng để tạo ra MTLT thực tế.

- ✓ Sự phát triển của MTLT hiện đại: MTLT hiện đại nhất hiện nay là Google's Sycamore [5], có khả năng tính toán vượt trội so với MTTT. Đây là một bước tiến lớn trong lĩnh vực MTLT và mở ra nhiều triển vọng trong việc ứng dụng của nó.

Những thành tựu đó đã đánh dấu một bước tiến lớn trong lĩnh vực MTLT, mở ra nhiều triển vọng và cơ hội cho việc phát triển và ứng dụng trong tương lai.

3.1.3. Các thành tựu đáng chú ý của các công ty và tập đoàn

Một trong những thành tựu đáng chú ý nhất của MTLT là quá trình đạt được quantum supremacy, tức là khả năng của MTLT vượt trội hơn so với MTTT trong một nhiệm vụ cụ thể [6], [9]. Thành tựu đầu tiên trong lĩnh vực này thuộc về Google vào năm 2019, khi họ đã sử dụng một MTLT 54 qubit để giải một bài toán phức tạp trong thời gian ngắn hơn so với MTTT [5]. Tuy nhiên, có những tranh cãi xung quanh việc xác định rõ ràng của khái niệm quantum supremacy [10], [11], [28].

IBM cũng đã đạt được quantum supremacy vào năm 2020 với một MTLT 65 qubit [11]. Công ty này đã sử dụng máy tính của mình để giải một bài toán liên quan đến phân tích ngôn ngữ tự nhiên với độ chính xác cao hơn so với các giải pháp truyền thống.

Ngoài Google và IBM, nhiều công ty và tổ chức khác cũng đang nỗ lực để đạt được quantum supremacy và phát triển những ứng dụng thực tiễn của MTLT. Ví dụ, vào năm 2020, Honeywell đã công bố một MTLT 6 qubit với độ chính xác cao hơn so với các MTLT cùng cấp độ. Còn Alibaba và Microsoft đang phát triển các MTLT với số lượng qubit lớn hơn [12]. Các thành tựu trên đang mở ra một tương lai rực rỡ cho lĩnh vực MTLT và nhiều ứng dụng mới có thể được tạo ra trong tương lai gần.

3.2. Nguyên lý hoạt động của MTLT

3.2.1. Các nguyên tắc hoạt động của MTLT

MTLT hoạt động dựa trên một số nguyên tắc vật lý cơ bản, bao gồm nguyên lý siêu dẫn, nguyên lý bù trừ và nguyên lý siêu vị nhân [14] – [16].

Nguyên lý siêu dẫn (superconductivity) là nguyên tắc vật lý mô tả sự dẫn điện hoàn toàn của vật liệu khi được làm lạnh đến một nhiệt độ rất thấp. Điều này cho phép các dòng điện chạy qua vật liệu mà không gặp phải sự trở kháng. Nguyên tắc này được sử dụng trong các quantum bit (qubit) của MTLT để giữ trạng thái của qubit với độ chính xác cao.

Nguyên lý bù trừ (quantum entanglement) là nguyên tắc vật lý mô tả sự liên kết giữa các hạt với nhau, dù chúng có thể ở cách xa nhau đến hàng trăm nghìn kilômét. Khi hai qubit liên kết với nhau thông qua nguyên tắc này, thì sự thay đổi của một qubit sẽ ảnh hưởng đến trạng thái của qubit kia, bất kể khoảng cách giữa hai qubit đó.

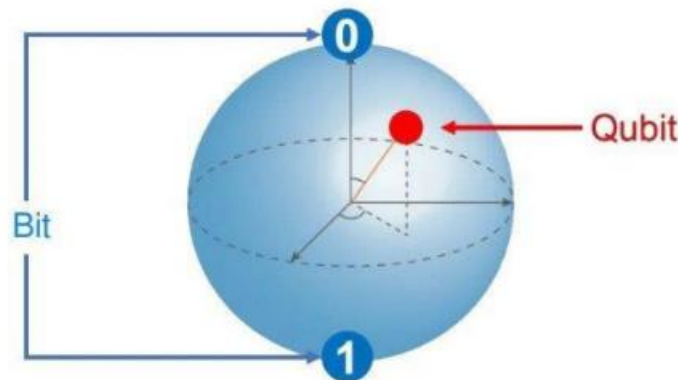
Nguyên lý siêu vị nhân (quantum tunneling) là nguyên tắc vật lý mô tả sự xuyên qua của các hạt qua một vật liệu mà không gặp sự trở kháng. Điều này cho phép qubit có khả năng chuyển trạng thái một cách rất nhanh chóng, mà không cần mất thời gian để vượt qua các vật liệu giữa.

Các nguyên tắc này tạo nên cơ sở cho sự hoạt động của MTLT, giúp nó có thể giải quyết các bài toán phức tạp một cách nhanh chóng hơn so với MTTT.

3.2.2. Thành phần cấu tạo của MTLT

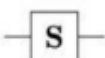
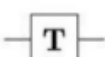
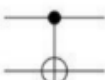
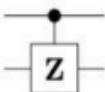
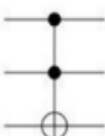
MTLT được tạo ra để thực hiện tính toán bằng cách sử dụng các phép toán trên các trạng thái lượng tử. Các thành phần cấu tạo của MTLT bao gồm qubit, quantum gate và quantum register [1], [6], [16], [19], [20], [22].

✓ **Qubit:** Qubit (quantum bit) là đơn vị cơ bản của MTLT và tương đương với bit trong máy tính cổ điển. Tuy nhiên, qubit không chỉ mang giá trị 0 hoặc 1 như bit nhị phân, mà có thể tồn tại trong một trạng thái siêu dẫn của 0 và 1 đồng thời (superposition) (xem minh họa trên hình 1). Điều này cho phép qubit thực hiện các tính toán đồng thời trên nhiều giá trị hơn là một giá trị duy nhất như trên máy tính cổ điển.



Hình 1. Minh họa Qubit

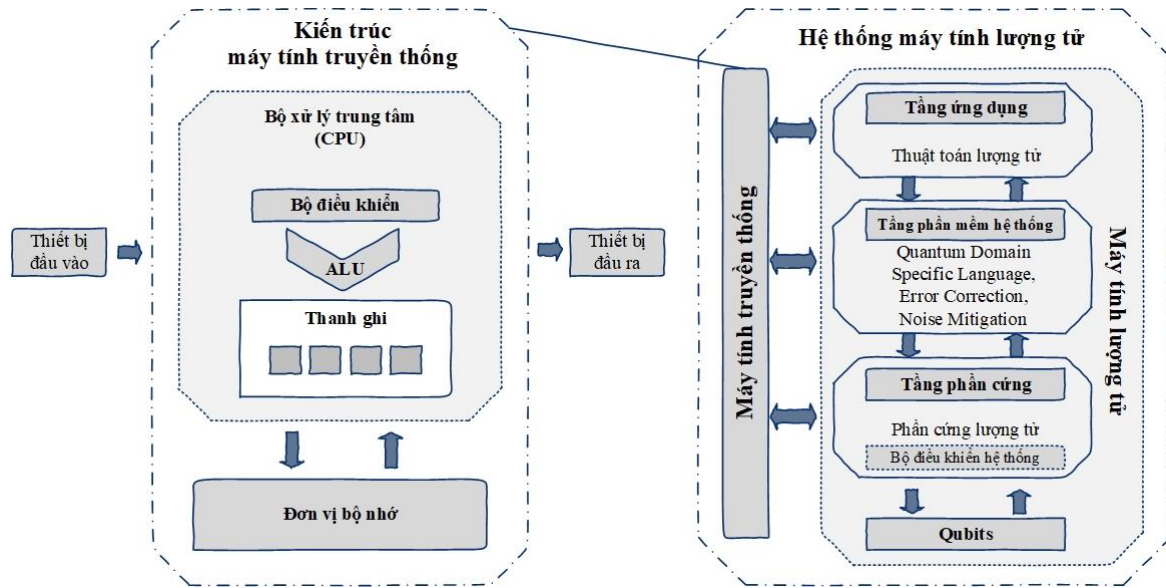
✓ **Quantum gate:** là các phép toán được sử dụng để thực hiện các tính toán trên qubit. Hình 2 mô tả tên các phép toán lượng tử tương ứng với các quantum gate và ma trận toán học tương ứng. Các quantum gate có thể được sử dụng để biến đổi trạng thái của qubit hoặc để tạo ra sự tương tác giữa các qubit. Các quantum gate phổ biến bao gồm X-gate, Y-gate, Z-gate, Hadamard gate, CNOT gate, SWAP gate, Toffoli gate và một số các cổng khác.

Phép toán	Tên cổng tương ứng	Ma trận
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Hình 2. Minh họa một số cổng lượng tử và phép toán tương ứng

✓ *Quantum register*: là tập hợp các qubit được sử dụng để lưu trữ và thực hiện các tính toán. Quantum register có thể có từ một đến hàng trăm qubit, tùy thuộc vào ứng dụng cụ thể.

Các thành phần này cùng hoạt động để tạo ra sức mạnh tính toán của MTLT. Khi các qubit được kết hợp với các quantum gate và được tổ chức trong quantum register, các tính toán lượng tử phức tạp có thể được thực hiện. Ngoài các thành phần khác biệt như trình bày trên của MTLT, các thành phần cấu tạo cơ bản khác của một hệ thống tính toán được giới thiệu và minh họa trong [36] (xem hình 3).



Hình 3. Minh họa MTTT và MTLT [36]

3.2.3. So sánh giữa MTLT và MTTT

MTLT và MTTT đều là những công cụ để xử lý thông tin, tuy nhiên chúng khác nhau về cách thức hoạt động và cách tiếp cận vấn đề. Bảng 1 trình bày sự khác nhau theo một số cách tiếp cận chính tạo ra sự khác biệt vượt trội như: cách biểu diễn thông tin, thao tác lưu trữ, phương pháp giải quyết bài toán.

Bảng 1. So sánh sự khác biệt giữa MTLT và MTTT

Nội dung	MTTT	MTLT
Cách biểu diễn thông tin	- Sử dụng hệ thống nhị phân để biểu diễn thông tin dưới dạng các bit 0 và 1.	- Sử dụng các qubit để biểu diễn thông tin. Các qubit có trạng thái superposition, tức có thể đồng thời mang các giá trị 0 và 1 [1] – [6], [13]. - Cung cấp sức mạnh tính toán lớn hơn [1] – [6], [13].
Thao tác và lưu trữ thông tin	- Thông tin được xử lý dưới dạng các phép toán logic cơ bản, thực hiện trên các bit.	- Thông tin được xử lý bằng cách sử dụng các cổng lượng tử như cổng Hadamard, cổng CNOT, cổng Toffoli, v.v. [1] – [6], [13]. - Ngoài ra, việc lưu trữ thông tin trong MTLT rất khó khăn, do sự phân tán và mất mát thông tin trong quá trình xử lý [1] – [6], [13].
Phương pháp giải quyết bài toán	- Việc giải quyết các bài toán phức tạp thường phải dựa cách hiệu quả hơn bằng cách sử dụng các thuật toán trên sức mạnh tính toán của bộ nhớ, và thường có thể mất nhiều thời gian để giải quyết các bài toán lớn.	- Các bài toán phức tạp có thể được giải quyết một cách hiệu quả hơn bằng cách sử dụng các thuật toán lượng tử như thuật toán Grover, thuật toán Shor, v.v. [1] – [6], [13], [17], [18]. - Việc lập trình cho MTLT cũng rất phức tạp và đòi hỏi kiến thức chuyên sâu về vật lý lượng tử [1] – [6], [13].

Tóm lại, MTLT và MTTT đều có sức mạnh và hạn chế riêng, có thể được sử dụng để giải quyết các bài toán khác nhau. Tuy nhiên, vì tính đặc biệt của MTLT, nó có thể giải quyết các bài toán phức tạp và lớn hơn nhiều so với MTTT. Song việc phát triển và sử dụng MTLT vẫn còn rất khó khăn và đòi hỏi sự đầu tư lớn về kỹ thuật và tài chính. Hiện nay, MTLT được sử dụng trong nhiều lĩnh vực như tài chính, y học, và khoa học vật lý. Với sự phát triển của công nghệ, các ứng

dụng của MTLT dự kiến sẽ tiếp tục mở rộng và đóng góp vào sự phát triển của nhiều lĩnh vực khác nhau.

3.3. Ứng dụng của MTLT

3.3.1. Ứng dụng trong khoa học

MTLT có tiềm năng để thực hiện các phép tính phức tạp hơn rất nhiều so với máy tính cổ điển, và điều này đã mở ra nhiều cánh cửa cho các ứng dụng mới trong nhiều lĩnh vực khoa học. Sau đây là một số ví dụ về ứng dụng của MTLT:

- ✓ Nghiên cứu vật lý: MTLT có thể được sử dụng để mô phỏng các hiện tượng vật lý phức tạp, như quá trình tương tác giữa các hạt cơ bản trong vật chất [1], [14]. Nó có thể giúp các nhà khoa học hiểu sâu hơn về các hiện tượng vật lý phức tạp và phát triển các vật liệu mới.

- ✓ Nghiên cứu hóa học: MTLT có thể giúp các nhà hóa học tìm ra các phân tử và chất mới với tính chất đặc biệt, bao gồm cả các vật liệu siêu dẫn và phân tử dược phẩm. Nó có thể mô phỏng các phản ứng hóa học và giúp đưa ra dự đoán về tính chất của các chất mới [13], [21], [22].

- ✓ Nghiên cứu sinh học: MTLT có thể giúp giải mã các cấu trúc phức tạp của các phân tử sinh học, như protein và DNA, và dự đoán cách chúng tương tác với các phân tử khác [12]. Nó có thể giúp giải quyết các vấn đề liên quan đến thiết kế các phân tử dược phẩm, chẩn đoán bệnh và phát triển các phương pháp điều trị mới [14].

- ✓ Nghiên cứu khoa học vũ trụ: MTLT có thể được sử dụng để mô phỏng các hiện tượng vũ trụ phức tạp, như tạo hình của các hành tinh và vũ trụ trong quá trình hình thành. Nó cũng có thể giúp giải quyết các vấn đề liên quan đến việc tìm kiếm sự sống ở ngoài Trái Đất [1], [6].

Tuy nhiên, việc sử dụng MTLT để giải quyết các bài toán thực tế vẫn còn rất mới và đang tiếp tục được nhiều nhà khoa học nghiên cứu.

3.3.2. Ứng dụng trong kinh doanh

MTLT là công nghệ tiên tiến có thể mang lại lợi ích lớn cho lĩnh vực kinh doanh. Dưới đây là một số ứng dụng của MTLT trong lĩnh vực này:

- ✓ Bảo mật thông tin: MTLT có khả năng xử lý các thuật toán mã hóa bảo mật thông tin nhanh hơn so với máy tính cổ điển. Vì vậy, các công ty tài chính và các tổ chức đòi hỏi tính bảo mật cao như ngân hàng, chính phủ, quân đội đã sử dụng MTLT để bảo vệ thông tin của mình. Các thuật toán như thuật toán Shor có thể phá vỡ các thuật toán mã hóa bảo mật thông tin phổ biến như RSA và ECC. Tuy nhiên, các thuật toán mã hóa dựa trên nguyên lý của MTLT như Quantum Key Distribution (QKD) có thể được sử dụng để bảo mật thông tin một cách an toàn [1], [6], [25], [27], [29].

- ✓ Tối ưu hóa tài chính: MTLT có khả năng tính toán nhanh hơn và hiệu quả hơn so với máy tính cổ điển. Vì vậy, nó có thể được sử dụng để giải quyết các vấn đề tối ưu hóa trong lĩnh vực tài chính, bao gồm tối ưu hóa danh mục đầu tư, phân bổ tài sản và quản lý rủi ro [11], [13], [14], [34], [35]. Các công ty tài chính lớn như JPMorgan Chase, Goldman Sachs, và Barclays đang sử dụng MTLT để cải thiện hoạt động của họ.

- ✓ Phân tích dữ liệu: MTLT có khả năng xử lý các thuật toán phân tích dữ liệu lớn nhanh hơn và hiệu quả hơn so với MTTT [14], [18]. Vì vậy, nó có thể được sử dụng để phát hiện các mô hình và xu hướng trong dữ liệu, giúp các doanh nghiệp đưa ra quyết định dựa trên những thông tin chính xác hơn.

- ✓ Dự đoán thị trường: là một trong những ứng dụng tiềm năng của MTLT trong lĩnh vực kinh doanh [31] – [35]. Các nhà đầu tư có thể sử dụng MTLT để phân tích dữ liệu từ thị trường tài chính và dự đoán giá cổ phiếu, ngoại tệ, hàng hóa và các loại tài sản khác. MTLT có thể giúp tăng độ chính xác và tốc độ của việc dự đoán thị trường, đồng thời giảm thiểu rủi ro và tổn thất [14]. Một trong những ứng dụng tiêu biểu của MTLT trong dự đoán thị trường là giải phương trình Black-Scholes, được sử dụng để định giá các tùy chọn tài chính. Giải phương trình này trên MTLT có thể giúp tăng độ chính xác và tốc độ tính toán, giúp các nhà đầu tư đưa ra quyết định

đúng dẫn về đầu tư tài chính [13]. Một số công ty đã bắt đầu sử dụng MTLT để phân tích dữ liệu và dự đoán thị trường, bao gồm JP Morgan, Goldman Sachs và Morgan Stanley [11]. Tuy nhiên, việc sử dụng MTLT trong dự đoán thị trường vẫn đang ở giai đoạn đầu, cần có thêm nhiều nghiên cứu và phát triển để phát huy tối đa tiềm năng của công nghệ này.

3.3.3. Ứng dụng trong chính phủ và quân đội

MTLT đang trở thành một công cụ quan trọng trong chính phủ và quân đội với các ứng dụng rộng rãi, từ mã hóa thông tin cho đến phát hiện gián điệp và dự báo khủng bố. Dưới đây là một số ứng dụng của MTLT trong lĩnh vực này:

✓ *Mã hóa thông tin*: MTLT có thể được sử dụng để tạo ra các mã khóa mạnh hơn và an toàn hơn cho việc bảo vệ thông tin nhạy cảm [15]. Các giải thuật mã hóa dựa trên nguyên tắc của lý thuyết thông tin lượng tử có thể giúp bảo vệ thông tin khỏi các cuộc tấn công bằng cách sử dụng các thuật toán phức tạp hơn so với các giải thuật mã hóa truyền thống.

✓ *Phát hiện gián điệp*: MTLT cũng có thể được sử dụng để phát hiện gián điệp trong các mạng liên lạc và hệ thống máy tính của chính phủ và quân đội [13]. Các giải thuật dựa trên thông tin lượng tử có thể giúp phát hiện các cuộc tấn công từ gián điệp một cách hiệu quả hơn.

✓ *Dự báo khủng bố*: MTLT có thể được sử dụng để dự báo các hoạt động khủng bố và xác định các mối đe dọa tiềm tàng [14]. Bằng cách sử dụng MTLT, các nhà nghiên cứu có thể phân tích các dữ liệu phức tạp một cách nhanh chóng và chính xác, đưa ra các kịch bản và dự đoán về các hoạt động khủng bố trong tương lai. Các quyết định về việc triển khai các biện pháp phòng ngừa và đối phó cũng có thể được đưa ra dựa trên các dữ liệu và dự báo này.

✓ *Nghiên cứu vũ khí mới*: MTLT có thể giúp giảm thời gian và chi phí để nghiên cứu và phát triển các vũ khí mới [12], [13]. Các giải thuật MTLT có thể được sử dụng để mô phỏng các phản ứng hạt nhân và các hiện tượng vật lý phức tạp khác, giúp các nhà nghiên cứu có thể đưa ra các kết quả nhanh hơn và chính xác hơn.

3.4. Thách thức, cơ hội, tầm nhìn của MTLT

3.4.1. Thách thức của MTLT

MTLT đã đạt được nhiều thành tựu trong những năm gần đây và tiềm năng của nó là vô tận. Tuy nhiên, vẫn còn nhiều thách thức cần được giải quyết để đưa MTLT trở thành một công nghệ quan trọng trong tương lai. Một trong những thách thức lớn nhất của MTLT là độ ổn định của qubit [12], [14], [30], [32]. Qubit rất nhạy cảm với các tác động bên ngoài như tia X, nhiệt độ và tương tác với các qubit khác, dẫn đến sự mất mát và lỗi tính toán. Điều này đặt ra một thách thức lớn trong việc thiết kế và xây dựng các thiết bị MTLT.

Ngoài ra, độ chính xác của kết quả tính toán cũng là một thách thức đáng kể. Mặc dù MTLT có thể giải quyết các bài toán phức tạp nhanh hơn so với máy tính cổ điển, nhưng kết quả tính toán của nó có thể không chính xác 100%. Điều này đặc biệt quan trọng đối với các ứng dụng trong lĩnh vực tài chính và khoa học vật liệu, nơi độ chính xác là yếu tố quan trọng để đưa ra quyết định chính xác [13], [14].

Cuối cùng, khả năng mở rộng của hệ thống cũng là một thách thức. Hiện tại, MTLT chỉ có thể giải quyết một số bài toán nhất định vì số lượng qubit và quá trình đồng bộ hóa giữa chúng có giới hạn [6], [14], [34]. Để mở rộng khả năng giải quyết của MTLT, các nhà khoa học đang nghiên cứu các cách thức để kết hợp các hệ thống MTLT với nhau và tăng số lượng qubit.

MTLT đang đối mặt với nhiều thách thức trong quá trình phát triển và vẫn còn nhiều công việc cần được thực hiện để đưa nó trở thành một công nghệ thực sự phát triển và mở rộng. Tuy nhiên, với tiềm năng vô tận của nó, các nhà khoa học vẫn đang nỗ lực để giải quyết các thách thức này để đưa MTLT trở thành một công cụ phổ biến trong các lĩnh vực khác nhau, từ khoa học cơ bản đến ứng dụng thực tiễn.

3.4.2. Cơ hội của MTLT

MTLT là một công nghệ đang được nghiên cứu rất nhiều trong những năm gần đây. Nó có tiềm năng rất lớn để thay đổi thế giới của chúng ta và mang lại những cơ hội đáng kể. Dưới đây là một số ví dụ về cơ hội mà MTLT có thể mang lại:

✓ *Tăng tốc các phát minh khoa học:* MTLT có thể giúp tăng tốc quá trình nghiên cứu và phát triển các phát minh khoa học. Ví dụ, trong lĩnh vực vật lý, MTLT có thể giúp mô phỏng các hiện tượng tự nhiên phức tạp hơn và giải quyết các bài toán mà các MTTT không thể giải quyết được [1], [13], [33] – [35].

✓ *Cải thiện hiệu quả tài chính:* MTLT có thể giúp cải thiện hiệu quả tài chính bằng cách giúp tối ưu hóa các quyết định đầu tư và quản lý rủi ro tài chính. Ví dụ, MTLT có thể giúp tính toán mô hình giá tài sản phức tạp và giúp các nhà đầu tư đưa ra quyết định đầu tư chính xác hơn [1], [14], [25] – [29].

✓ *Giải quyết các vấn đề khó khăn trong thế giới thực:* MTLT có thể giúp giải quyết các vấn đề khó khăn trong thế giới thực, bao gồm nghiên cứu về sự đa dạng sinh học, phát hiện các tác nhân gây bệnh, tối ưu hóa lộ trình giao thông và quản lý nguồn nước. Ví dụ, MTLT có thể giúp phân tích dữ liệu gen để tìm ra các phương pháp điều trị bệnh ung thư hiệu quả hơn [1], [4], [6].

Như vậy, MTLT là một công nghệ đầy tiềm năng và có thể mang lại nhiều cơ hội cho hầu hết các lĩnh vực trong tương lai. Tuy nhiên, vẫn còn rất nhiều thách thức cần phải vượt qua để đạt được những tiến bộ đáng kể và tận dụng được toàn bộ tiềm năng của công nghệ này.

3.4.3. Tầm nhìn

MTLT đang trên đà phát triển mạnh mẽ và trong tương lai, có tiềm năng lớn để đưa công nghệ tính toán lên một bước phát triển mới [31] – [35]. Chúng ta có thể mong đợi các thiết bị lượng tử có độ chính xác và độ mở rộng cao hơn, cho phép xử lý các bài toán phức tạp hơn và đưa ra dự đoán chính xác hơn trong nhiều lĩnh vực khác nhau. Điều quan trọng là việc nghiên cứu và phát triển MTLT sẽ đóng vai trò quan trọng trong tương lai của khoa học và công nghệ [33] – [34]. Nó có thể giúp chúng ta giải quyết các bài toán khoa học và kỹ thuật khó khăn hơn, từ nghiên cứu vật lý và hóa học đến tối ưu hóa tài chính và dự đoán thị trường. Ngoài ra, MTLT còn có thể được sử dụng để tăng tốc quá trình phát minh và phát triển sản phẩm mới, từ thuốc chữa bệnh đến các vật liệu tiên tiến. Bằng cách sử dụng MTLT để mô phỏng các quá trình vật lý và hóa học, chúng ta có thể tìm ra các giải pháp tối ưu và giảm thiểu thời gian và chi phí cho các quá trình thử nghiệm.

MTLT có tiềm năng lớn để đưa khoa học và công nghệ lên một tầm mới. Sự phát triển và tiến bộ trong lĩnh vực này sẽ đóng góp rất lớn cho việc giải quyết các vấn đề khó khăn trong thế giới thực và đưa ra những giải pháp mới cho những thách thức lớn của xã hội.

4. Kết luận

Trong bài báo này, chúng tôi đã cung cấp một cái nhìn tổng quan về MTLT bao gồm: lịch sử, nguyên lý hoạt động, cấu tạo, ứng dụng và thách thức. MTLT là một lĩnh vực đầy tiềm năng và đang phát triển rất nhanh chóng, với nhiều ứng dụng tiềm năng trong khoa học, kinh doanh và quân sự, v.v. Tuy nhiên, còn rất nhiều thách thức cần phải được giải quyết để đưa MTLT vào ứng dụng thực tế một cách hiệu quả.

TÀI LIỆU THAM KHẢO/ REFERENCES

- [1] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," *ACM Computing Surveys (CSUR)*, vol. 32, pp. 301-325, 01 September 2000, doi: 10.1145/367701.367709.
- [2] J. R. Mandel, "Quantum Computing: Resolving Myths, From Physics to Metaphysics," College of Science and Mathematics, Physics Department, March 2021. [Online]. Available: <https://digitalcommons.calpoly.edu/physsp/197/>. [Accessed Jan. 8, 2023].
- [3] R. D. Wolf, "Quantum computing: Lecture notes," *QuSoft*, CWI and University of Amsterdam, vol. 5, pp. 1-12, 2019, doi: 10.48550/arXiv.1907.09415.

- [4] M. Steffen, D. P. DiVincenzo, J. M. Chow, T. N. Theis, and M. B. Ketchen, "Quantum computing: An IBM perspective," *IBM Journal of Research and Development*, vol. 55, no. 5, pp. 1-11, 2011.
- [5] V. H. T. Huynh and T. M. Truong "The development of quantum computing in the past 20 years has been remarkable," *Nam Can Tho University - Journal of Science and Development Economics*, no. 12, pp. 35-47, 2021.
- [6] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nature Photonics*, vol. 3, pp. 1-2, 2009.
- [7] G. Kalai, Y. Rinott, and T. Shoham, "Google's 2019 Quantum Supremacy Claims: Data, Documentation, and Discussion," *Quantum Physics; Computational Complexity*, vol. 3, pp. 455-463, January 25, 2023, arXiv:2210.12753.
- [8] M.-H. Yung, "Quantum supremacy," *National Science Review*, vol. 6, no. 1, pp. 22-23, January 2019, doi: 10.1093/nsr/nwy072.
- [9] S. T. Marella, and H. S. K. Parisa, "Introduction to quantum computing," University of Leicester, UK, *Quantum Computing and Communications*, vol. 112, pp. 1-18, 2020.
- [10] E. Togan, Y. Chu, A. S. Trifonov, L. Jiang, J. Maze, L. Childress, M. V. G. Dutt, A.S. Sorensen, P.R. Hemmer, A.S. Zibrov, and M. D. Lukin, "Quantum entanglement between an optical photon and a solidstate spin qubit," *Nature*, vol. 466,, pp. 730–734, 2010.
- [11] E. Farhi, J. Goldstone, S. Gutmann, and H. Neven, "Quantum algorithms for fixed qubit architectures," Center for Theoretical Physics Massachusetts Institute of Technology Cambridge, MA 02139, vol. 1, 2017, arXiv:1703.06199.
- [12] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, and E. Jeffre, "Logic gates at the surface code threshold: Superconducting qubits poised for fault-tolerant quantum computing," *Nature*, vol. 508, pp.500–503, 2014.
- [13] G. J. Mooney, G. A. L. White, C. D. Hill, and L. C. L. Hollenberg, "Whole-Device Entanglement in a 65-Qubit Superconducting Quantum Computer," *Advanced Quantum*, vol. 4, no.10, pp. 1-11, October 2021, doi: 10.1002/qute.202100061.
- [14] R. Orús, S. Mugel, and E. Lizaso, "Quantum computing for finance: Overview and prospects," *Reviews in Physics*, vol. 4, November 2019, doi: 10.1016/j.revip.2019.100028.
- [15] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, "Quantum computing on encrypted data," *Nature Communications*, no. 3074, pp. 1-6, 2014.
- [16] G. Smith and J. Yard, *Quantum Computing: Progress and Prospects*, Washington, DC: The National Academies Press, 2019, doi: 10.17226/25196.
- [17] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca "Quantum algorithms revisited," *Proceedings of the Royal Society of London, Series A*, vol. 454, no. 1969, January 1998, doi: 10.1098/ rspa.1998.0164.
- [18] J. A. Cortese and T. M. Braje, "Loading Classical Data into a Quantum Computer," *arXiv:1803.01958*, 2018.
- [19] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A, Mathematical and Physical Sciences*, vol. 400, pp. 97–117, 1985.
- [20] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, pp. 553– 558, 1992.
- [21] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96*, 1996, pp. 212–219.
- [22] B. C. Hall, *Quantum Theory for Mathematicians. Graduate Texts in Mathematics*, Springer, New York, 2013.
- [23] S. Herbert, "On the depth overhead incurred when running quantum algorithms on near-term quantum computers with limited qubit connectivity," *Quantum Inf. Comput.*, vol. 20, pp. 787–806, 2018.
- [24] J. D. Hidary, *Quantum Computing: An Applied Approach*, Springer, 2019.
- [25] A. Jacquier and Kondratyev, *Quantum Machine Learning and Optimisation in Finance: On the Road to Quantum Advantage*, Packt Publishing, 2022.
- [26] P. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing*, Oxford University Press, 2007.
- [27] B. T. Lenahan, *Quantum Boost: Using Quantum Computing to Supercharge Your Business*, Aquitaine Innovation Advisors, May 2021.

-
- [28] F. Leymann and J. Barzen, "The bitter truth about gate-based quantum algorithms in the NISQ era," *Quantum Science and Technology*, vol. 5, no. 4, 2020, Art. no. 044007.
- [29] D. Herman, C. Googin, X. Liu, A. Galda, I. Safro, Y. Sun, M. Pistoia, and Y. Alexeev "A Survey of Quantum Computing for Finance," *Computational Finance*, vol. 4, pp. 1-39, 2022, arXiv:2201.02773.
- [30] T. Itoko, R. H. Putra, T. Imamichi, and A. Matsuo, "Optimization of Quantum Circuit Mapping using Gate Transformation and Commutation," *ArXiv: abs/1907.02686*, 2019.
- [31] Markets and Markets, "Global Quantum Computing Software Market by Component (Software, Services), Deployment Mode (Cloud, On-Premises), Organization Size, Technology, Application (Optimization, Simulation), Vertical (Bfsi, Government), and Region - Forecast to 2026", 2021. [Online]. Available: <https://www.researchandmarkets.com/reports/5387515/global-quantum-computing-software-market-by>. [Accessed Feb. 10, 2023].
- [32] QYResearch, "Global Quantum Computing Market Research Report 2020-2025," [Online]. Available: <https://www.fortunebusinessinsights.com/information-and-technology-industry>. [Accessed Feb. 10, 2023].
- [33] ReportOcean, "Global quantum computing market size study & forecast, by offering, by deployment, by application, by technology, by end-use industry and regional analysis, 2022-2029," [Online]. Available: https://reportocean.us/sample-request/category_slug/Global-Quantum-Computing-Market/report_id/bzwt1639. [Accessed Feb. 10, 2023].
- [34] Wintergreen Research, "Quantum Computing: Market Shares, Strategies, and Forecasts, Worldwide, 2019 to 2025," [Online]. Available: <https://apnews.com/article/technology-business-c3dc18d422304ea381d80f1f2da179f3>. [Accessed Feb. 10, 2023].
- [35] IMARC Group, "Quantum Computing Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2020-2025," [Online]. Available: <https://www.fortunebusinessinsights.com/quantum-computing-market-104855>. [Accessed Feb. 10, 2023].
- [36] R. Riétche, C. Dremel, S. Bóch, L. Steinacker, M. Meckel, and J-M. Leimeister, "Quantum computing," *Electronic Market*, no. 32, pp. 2525-2536, 2022, doi: 10.1007/s12525-022-00570-y.