JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Are Quantum Computers the Future of fast Computation

Prathamesh Valmik Patil

paddypatil2000@gmail.com

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

1. ABSTRACT

Quantum computing has become a hot topic in recent years. Devices used for quantum computing are quantum computing. A quantum computer is a machine that uses properties of quantum physics to store data and perform computations. This is very beneficial for certain tasks where even the best supercomputers can perform much better. Traditional computers, including smartphones and laptops, encode information into binary "bits" of 0s or 1s. In quantum computers, the basic unit of storage is the quantum bit (qubit).

Although there have been some successful developments in quantum computing technology, a lot of research and development must be done before quantum computing becomes viable as a mainstream technology, and why this potential will never be realized. There is debate about what is not achieved.The proposed research focuses on cybersecurity – will quantum computing break cybersecurity?

2. INTRODUCTION

Quantum computing is a kind of computation that harnesses the collective homes of quantum states, such as superposition, interference, and entanglement, to carry out calculations. The gadgets that carry out quantum computations are regarded as quantum computers.

[1] They are believed with a view to clear up certain computational problems, such as integer factorization (which underlies RSA encryption), appreciably quicker than classical computers. The take a look at of quantum computing is a subfield of quantum records science. Expansion is anticipated withinside the following couple of years[when?] as the sphere shifts closer to real-international use in pharmaceutical, facts safety and different applications.

[2] Quantum computing started out in 1980 whilst physicist Paul Benioff proposed a quantum mechanical version of the Turing machine.

[3] Richard Feynman and Yuri Manin later advised that a quantum laptop had the ability to simulate matters a classical laptop couldn't feasibly do.

[4] In 1994, Peter Shor developed a quantum algorithm for factoring integers with the ability to decrypt RSA-encrypted communications.

[5] Despite ongoing experimental development for the reason that overdue 1990s, maximum researchers trust that "fault-tolerant quantum computing [is] nonetheless a as an alternative remote dream.

[6] In current years, funding in quantum computing studies has extended withinside the public and personal sectors. On 23 October 2019, Google AI, in partnership with the U.S. National Aeronautics and Space Administration (NASA), claimed to have accomplished a quantum computation that turned into infeasible on any classical laptop, however whether or not this declare turned into or remains legitimate is a subject of energetic research.

3. QUANTUM SUPERPOSITION

Superposition is the term used to describe a quantum state in which a particle can exist in multiple states at the same time, allowing quantum computers to see many different variables simultaneously. A qubit (or qubit) is the quantum mechanical analogue of a classical bit. In traditional arithmetic operations, information is encoded bitwise, where each bit has the value 0 or 1. In quantum computing, information is encoded in qubits. A qubit is a two-level quantum system whose two fundamental qubit states are usually written as |0⟩ and |1⟩. A qubit can be in the |0⟩ state, the |1⟩ state, or (as opposed to a conventional bit) a linear combination of both states. The name of this phenomenon is superposition.

A qubit can be a superposition of two fundamental states |0⟩ and |1⟩. When the qubit is measured (more precisely:

can only measure observables), the qubit collapses to one of its eigenstates, and the measurement reflects that state. For example, if a qubit is in a superposition state with equal weights, the measurement shows that the qubit will collapse into one of the two fundamental states |0⟩ and |1⟩ with 50% probability. |0⟩ is the state that is collapsed when measured to always result in 0. Similarly, |1⟩ always converts to 1.

Quantum superposition is fundamentally different from classical wave superposition. A quantum computer consisting of n qubits can exist in a superposition of 2n states.

From |000...0⟩ to |111...1⟩. In contrast, playing n tones all at different frequencies will only result in a superposition of n frequencies. The addition of classical waves scales linearly, and the superposition of quantum states is exponential.

4. QUANTUM COMPUTERS vs CLASSICAL COMPUTERS

Let's explore some of the main differences between quantum and classical computers.

Information processing:

While classical computers rely on transistors to represent binary 0s or 1s, quantum computers use qubits. Qubits follow the principle of superposition and can represent both 0 and 1 at the same time.

Performance:

Quantum computer performance increases exponentially with the number of linked qubits. This is unlike what happens in classical computing. Conventional computer performance increases linearly with the number of transistors.

Application:

Quantum computers are well suited for complex tasks such as optimization problems, data analysis and processing, and simulations. Traditional computers are better suited for everyday processing needs.

Building blocks:

Superconducting quantum interface devices (SQUIDs) or quantum transistors are the fundamental building blocks of quantum computers. Conventional computers use CMOS transistors. Information processing:

In quantum computing, data processing takes place in quantum processing units (QPUs), which are made up of interconnected qubits. In traditional computing, data is processed in a central processing unit (CPU), which consists of an arithmetic logic unit (ALU, processor registers, and control unit).

Information display:

Classical computers use bits, but quantum computers use qubits.

Speed:

Quantum computers can solve certain problems hundreds of millions of times faster than classical computers. For example, in 2019, Google's quantum computer, the world's most powerful supercomputer, performed a calculation that would have taken him 10,000 years in less than 4 minutes.

5. QUANTUM COMPUTING Vs CYBER SECURITY

Tomorrow's quantum computers are expected to be millions of times faster than the devices we use today. Therefore, if these powerful computers were actually built, the chances of their data being hacked are high.

Suppose you have a bank account. Assume only you and your bank have access to your information, have strong passwords, and can use two-factor authentication. You know that bank has a strong security system. So you can be confident that no one else can change your confidential data. In the future, when you log into your account, you will see your savings transferred elsewhere. how is that possible? What happened to passwords, bank security systems, and two-factor authentication?

This happened because hackers used quantum computers. The speed of quantum computers makes it easier for hackers to break security algorithms. This threat affects everything from bank accounts, military communications, confidential records, and valuable data.

6. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a technique that uses quantum physics to protect the distribution of symmetric cryptographic keys. Quantum cryptographic algorithms may be able to crack traditional cryptographic keys that are currently too complex for classical computers to crack. As engineers race to create the first advanced quantum computers, cybersecurity experts race to introduce new forms of encryption that protect against quantum hacking. This is called post-quantum cryptography, or PQC. In cryptography, post-quantum cryptography (also known as quantum-secure, quantum-secure, or quantum-resistant) refers to cryptographic algorithms (usually public-key algorithms) that are believed to be secure against cryptanalysis attacks by quantum computers. increase. . Experts are currently developing PQC solutions, but these need to be standardized and widely implemented. This may take years or decades. “Post-quantum cryptography is the best solution,” said Vermeer. "It's important to finish it on time."

7. GOOGLE’S QUANTUM COMPUTER

Google has officially announced that it has achieved quantum supremacy in a new article published in the journal Nature. Google says its 54-qubit Sycamore processor is the world's most powerful supercomputer, allowing him to perform calculations in 200 seconds that would have taken him 10,000 years. This means that computations involving generated random numbers are inherently impossible on conventional non-quantum computers. That extra processing power could help it accurately simulate molecules, hence nature, says Google. Being able to do so, this could help design better batteries, produce more carbon-efficient fertilizers, or develop more targeted medicines. Google also expects significant benefits for AI development from quantum computing.

8. FINDINGS

1.Quantum computing can change the world of computing.

2.Few people know about this computer.

3.People are ready to use these quantum computers.

4.Quantum computers are the future of high-speed computing.

5.Quantum cryptography can break traditional cryptography. However, there is a solution to this: PQC (Post Quantum Cryptography).

9. ACKNOWLEDGEMENT

I would like to express my sincere gratitude and respect to the many people who have supported and guided me thus far.

I would like to thank Professor Gauri Ansurkar for giving me research ideas. Throughout her work, she has greatly benefited from her regular critique and inspiration. We thank them for their guidance, encouragement, understanding, and insightful support in this research.

Finally, I would like to express my sincere gratitude to my parents and friends for their constant support and encouragement during my college years and throughout the process of researching and writing this thesis. Without her, this achievement would not have been possible. It was impossible. Thank you very much.

10. CONCLUSION

In this article, we have reviewed the principles, algorithms, and cybersecurity of quantum computing. While the fundamentals of the topic of quantum computing are well established, everything else necessary for future growth is being explored. Quantum computers have the potential to revolutionize computation by enabling them to solve certain types of classically unsolvable problems.

Quantum computers have the potential to be useful to society in various ways. Quantum computers can solve problems that are impossible or take an unrealistically long time (billion years) to solve with conventional computers. Quantum computers have the potential to change the world of computing.

It also has some drawbacks. Quantum cryptography can break traditional cryptography. Hackers can use quantum computers that can lead to cyberattacks.

As engineers race to create the first advanced quantum computers, cybersecurity experts race to introduce new forms of encryption that protect against quantum hacking. This is called post-quantum cryptography, or PQC. PQC is the best solution.

REFERENCES

[1] National Academy of Sciences, Engineering and Medicine (2019). Mullen, Emily. Horowitz, Mark (ed.). Quantum computing: Progress and Perspectives (2018). Washington DC. : National Academy Press

[2] “Scope of Corporate Research and Development”

[3] Benioff, Paul (1980). "Computers as physical systems: A microscopic quantum-mechanical Hamiltonian model of computers represented by Turing machines. Journal of Statistical Physics. 22 (5): 563-591.

[4] Feynman, Richard (June 1982). "Computer Physics Simulation" (PDF). International Journal of Theoretical Physics. 21 (6/7): 467-488.

[5] Manin, Yu. I (1980). Vychislimoe i nevychislimoe [predictable and unpredictable] (Russian). Sov.Radio. Pages 13-15. Archived from the original on 10 May 2013. Retrieved March 4, 2013.

[6] Mermin, David (28 March 2006). "Breaking RSA encryption with a quantum computer:

Shor's Factoring Algorithm" (PDF). Physics 481-681 Lecture Notes. Cornell University. Archived from the original (PDF) on 15 November 2012.

[7] Preskill, John (2018). "Quantum Computing in the NISQ Era and Beyond" Quantum 2: 79. ar Xiv

[8] "On 'quantum supremacy'". IBM research blog. October 22, 2019. Retrieved February 9, 2021. [9]https://www.newscientist.com/question/what-is-a-quantum-computer/#ixzz79BabR5Vg

[10] https://en.m.wikipedia.org/wiki/Quantum_computing

[11]https://www.google.com/amp/s/www.theverge.com/platform/amp/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor

[12]https://www.quantum-inspire.com/kbase/superposition-and-entanglement/

[13] https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html