Quantum Computing: Another Tech to Worry About?

Nicola Roberts-Lewis

Computers have revolutionized our world. From just initial calculation machines, computers now run almost every facet of our society. They drive our communication, our transportation, and our entertainment.[1] This technology that powers our lives is based on the same basic technology that was first used in computation in 1939. Just as they did then, computers now process using a binary numbering system, where everything is represented using 0 and 1, to process information.[2]

Quantum computers instead use qubits, where a particle, such as an electron, is used to represent either or both a 0 and a 1. Utilizing these particles, quantum computers can process data using an infinite and continuous number of states, known as a wave function, which allows for the potential to outperform classical computers.[3] Quantum computers have the potential to surpass traditional computers in a variety of areas, including the speed at which problems will be solved, enhanced simulations, and machine learning.[4] Practically, this translates to developments in cryptography and cybersecurity, drug discovery, and optimization of financial modeling and portfolios.[5] With all the potential of quantum computers, companies are investing big. Quantum technology start-ups had $2.35 billion in investments in 2022.[6] As of 2024, that number has jumped to $5 billion.[7]

Are Quantum Computers as Great as Everyone is Saying They Are?

Despite the theoretical prowess of quantum computers, there are a handful of barriers that inhibit quantum computers from making the big steps we are so excited about.

First, there is quite a bit of noise which inhibits quantum computers' accuracy. Noise is any disruption to the system, be it "a stray photon created by heat, a random signal from the surrounding electronics, or a physical vibration."[8] This noise affects the transmission of quantum information by altering/interrupting/disrupting the wave function, which will then produce incorrect results. [9] Researchers have approached the reduction of noise problem through both hardware and software solutions. For example, to ensure that temperature does not create any

---

[1] Satish Gill, *Impacts of Computers on Today's Society*, 2 INT'L J. OF CORE ENG'G AND MGMT. 1, 174 (2015).
[2] *Quantum Computing Vs. Classical Computing in One Graphic*, CB INSIGHTS (Feb. 2, 2021), https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/.
[3] *Id.*; David P. DiVincenzo, *Quantum Computation*, 270 SCIENCE 255, 255 (1995).
[4] Pwaveino Clarkson, *The Future of Quantum Computing: Potential Applications and Challenges*, MEDIUM (Jul. 22, 2023), https://medium.com/@pwaveino/the-future-of-quantum-computing-potential-applications-and-challenges-733f2158aa6c.
[5] *Id*.
[6] *Quantum Technology Sees Record Investments, Progress on Talent Gap*, MCKINSEY DIGITAL (Apr. 24, 2023), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap.
[7] Michael Brooks, *Quantum Computing Is Taking On Its Biggest Challenge: Noise*, MIT TECH. REV. (Jan. 4, 2024), https://www.technologyreview.com/2024/01/04/1084783/quantum-computing-noise-google-ibm-microsoft/.
[8]. *Id*.
[9] *How To Overcome Noise in Quantum Computation*, PHYS ORG (Apr. 6, 2023), https://phys.org/news/2023-04-noise-quantum.html.

noise, quantum computer circuits are chilled to near absolute zero.[10] Methods of optimal refrigeration is a subject of some researchers, because refrigeration carries its own costs.[11] From a software standpoint, researches have been focusing on developing qubits they liken to noise cancelling headphones.[12] These special qubits are designed/put into the computer with the sole purpose of monitoring noise and adjusting the qubits in the system.[13]

Second, the processors are not that big yet. Currently, quantum computers do not have enough qubits to achieve calculations that are more impressive than those done by traditional supercomputers.[14] Furthermore, some of the technologies to address noise, as discussed above, rely on ancillary qubits which cannot be used for the primary calculations. IBM's current largest quantum computer only has 433 qubits.[15] Currently, the technology is not mature enough to solve any practical problem; it is still a nascent stage of technology used by researchers. To achieve more efficient machines, continued academic and industrial research is needed.[16]

Why Should We Care?

Despite these issues, it is important for policy makers to be prepared for when the technology is viable. One reason for this concern is national security and internet security. Traditionally, any data transmitted over the internet, from banking transactions to military communications requires encryption to secure the information. Encryption essentially scrambles this data in a way that can only be read by a system that has the ability to unscramble it.

Our most secure transactions are encrypted in such a way that cannot be cracked with traditional super computers. For example, Advanced Encryption Standard (AES) is used for many of our secure online transactions, be it using Cloud services, online banking, or accessing Wi-Fi networks.[17] Additionally, AES is used by the U.S. government for their encryption needs.[18] With traditional supercomputers, it is estimated that it would take 1 billion years to crack the lowest level of AES encryption.[19] However, quantum computers have the predicted potential to "fundamentally undermine . . . encryption protocols."[20] The impacts of this possibility are difficult to comprehend. No banking transaction or personal information would be secure;

---

[10] Charles Q. Choi, *Electric Cooling Could Shrink Quantum Computers*, IEEE SPECTRUM (Sep. 12, 2023), https://spectrum.ieee.org/cryogenics.
[11] *Id*. (refrigeration in itself is difficult at these low of temperatures and has its own costs that are irrelevant of quantum computing).
[12] *Id*.; Sarah C.P. Williams, *'Noise-Cancelling' Qubits Developed at UChicago to Minimize Errors in Quantum Computers*, UNIV. OF CHICAGO PRITZKER SCH. OF MOLECULAR ENG'G (May 25, 2023), https://pme.uchicago.edu/news/noise-cancelling-qubits-developed-uchicago-minimize-errors-quantum-computers.
[13] Williams, *supra* note 12.
[14] Michael Brooks, IBM Wants to Build a 100,000-Qubit Quantum Computer, MIT Tech. Rev. (May 25, 2023), https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/.
[15] Davide Castelvecchi, *Are Quantum Computers About to Break Online Privacy?*, 613 Nature 221, 222 (2023).
[16] *Id*.
[17] Luke Probasco, *Encryption Requirements For Banks & Financial Services*, TOWNSEND SEC. DATA PRIV. BLOG (Apr. 25, 2017), https://info.townsendsecurity.com/encryption-requirements-for-banks-financial-services; *What is AES Encryption, and Why Is it Important?*, WINZIP, https://winzip.com/blog/enterprise/aes-encryption-explained/ (last visited Feb. 17, 2024).
[18] WinZip, *supra* note 18.
[19] Mohit Arora, *How Secure Is AES 128 and 256 Encrypting Against Brute Force Attacks?*, EE TIMES (May 7, 2012), https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/?_ga.
[20] Zach Montague, *The Race to Save Our Secrets From the Computers of the Future*, NEW YORK TIMES (Oct. 22, 2023), https://www.nytimes.com/2023/10/22/us/politics/quantum-computing-encryption.html.

sensitive miliary information such as intelligence, weapon design, and nuclear protocols would be accessible; and electricity grids would be affected.[21]

While this could easily be classified as yet another doomerism prophecy to the world, such as the rise of AI and global warming effects, this is a real threat that U.S. officials and other global powers are taking seriously.[22] This issue is different and maybe more important than AI regulation. We know AI is powerful, but regulators must take a wait-and-see approach to see the actual, realized effects. With quantum computers, there is an absolute possibility that these awful things could happen. Of course, this will not happen until the issues of noise and size, discussed earlier, are solved.[23] In addition to racing to develop their own quantum computers as a sort of weapon against others, the United States is also devoting research to new "quantum-resistant algorithms."[24] In 2022, the National Institute of Standards and Technology (NIST) announced the successful development of quantum-resistant algorithms.[25] This came after a six-year effort of cryptographers creating and testing new encryption methods that would be able to sustain an attack from a quantum computer.

This is not a call to stop quantum computing development. Even if it were, it is a bit late. Quantum computing possesses the ability to bring so many new innovations to the world. Not only are there significant advances that can be made in fields such as pharmaceuticals and machine learning with the advent of quantum computers, but scientific development should also not be stopped because of the possible negative effects.

---

[21] *Id*.
[22] *Id*.
[23] *See* Emily Conover, *Quantum Computers Could Break the Internet. Here's How to Save It*, SCIENCENEWS (Jun. 28, 2023), https://www.sciencenews.org/article/quantum-computers-break-internet-save (prediction that we are 15 years away from having the necessary qubits to crack encryption); *see also* Castelvecchi, *supra* note 15 (one million qubits needed to crack RSA, while the current largest quantum computer only has 433 qubits).
[24] Montague, *supra* note 21.
[25] *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, NIST (July 5, 2022), https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.