EXPLORE

INVB1447LV

Quantum Computing

What Are You Scared of?

John Yani Arrasjid
Regional Technical Officer, Broadcom

Tony Foster
Sr. Principal Engineering Technologist, Dell Technologies

#vmwareexplore #INVB1447LV

Disclaimer

- Certain information in this presentation may outline Broadcom's general product direction.
- This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product.
- This presentation is based on current information and resource allocations and is subject to change or withdrawal by Broadcom at any time without notice.
- The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.
- Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release.
- Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis.
- The information in this presentation is not deemed to be incorporated into any contract.

Overview and Objectives

Fear Quantum

- Overview of general quantum fears

Introduction to Quantum Computing

- Define and explain the basic principles of quantum computing.

Advances and Use Cases

- Explore recent advancements and specific industry applications.

Challenges and Risks

- Probe potential issues, risks, and challenges associated with quantum computing.

Quantum Sized Fear

Security Threats

Breaking existing encryption, putting sensitive data at risk.

Job Displacement

Automation and advanced problem-solving capabilities may lead to job losses in certain sectors.

Ethical Issues

Concerns about its misuse and the digital divide.

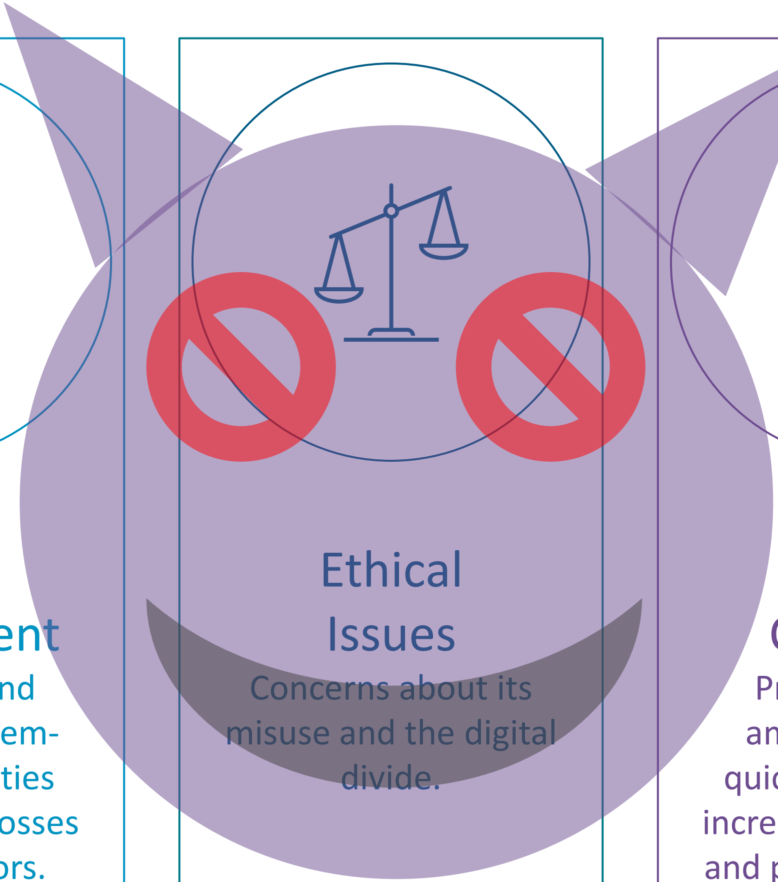
Privacy Concerns

Processing vast amounts of data quickly may lead to increased surveillance and privacy invasions.

Economic Disruption

Disruption to existing business models and new competitive dynamics.

Quantum Sized Fear



Security Threats

Breaking existing encryption, putting sensitive data at risk.

Job Displacement

Automation and advanced problem-solving capabilities may lead to job losses in certain sectors.

Ethical Issues

Concerns about its misuse and the digital divide.

Privacy Concerns

Processing vast amounts of data quickly may lead to increased surveillance and privacy invasions.

Economic Disruption

Disruption to existing business models and new competitive dynamics.

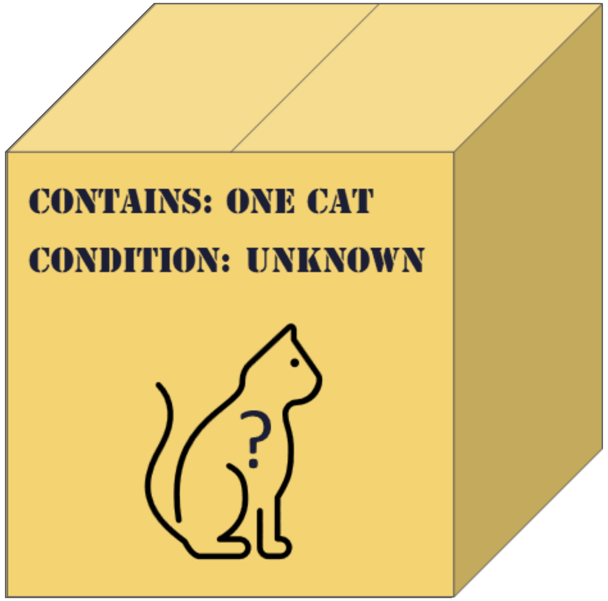
What is Quantum Computing?

Definition: Quantum computing leverages quantum mechanics principles to perform computations.

Foundation: Based on qubits, superposition, and entanglement instead of classical bits.

Potential: Offers exponential speedup for certain complex problems compared to classical computers.

Go Deeper: “Quantum Leap: The Ever-Changing Virtual Space of Quantum Computing” [VMTN3079LV] *VMware Explore 2023*, Arrasjid & Foster. https://www.wondernerd.net/quantum-leap-the-ever%E2%80%90changing-virtual-space-of-quantum-computing-vmtn3079lv/



Key Concepts: Qubits, Superposition, Entanglement

Qubits

- Basic unit of quantum information, analogous to classical bits but can exist in multiple states simultaneously.

Superposition

- Qubits can exist in multiple states at once, enabling parallel computation. (Schrodinger's Cat)

Entanglement

- Quantum particles become interconnected, with the state of one instantly influencing the state of another, regardless of distance.
  (Ripples on a pond)

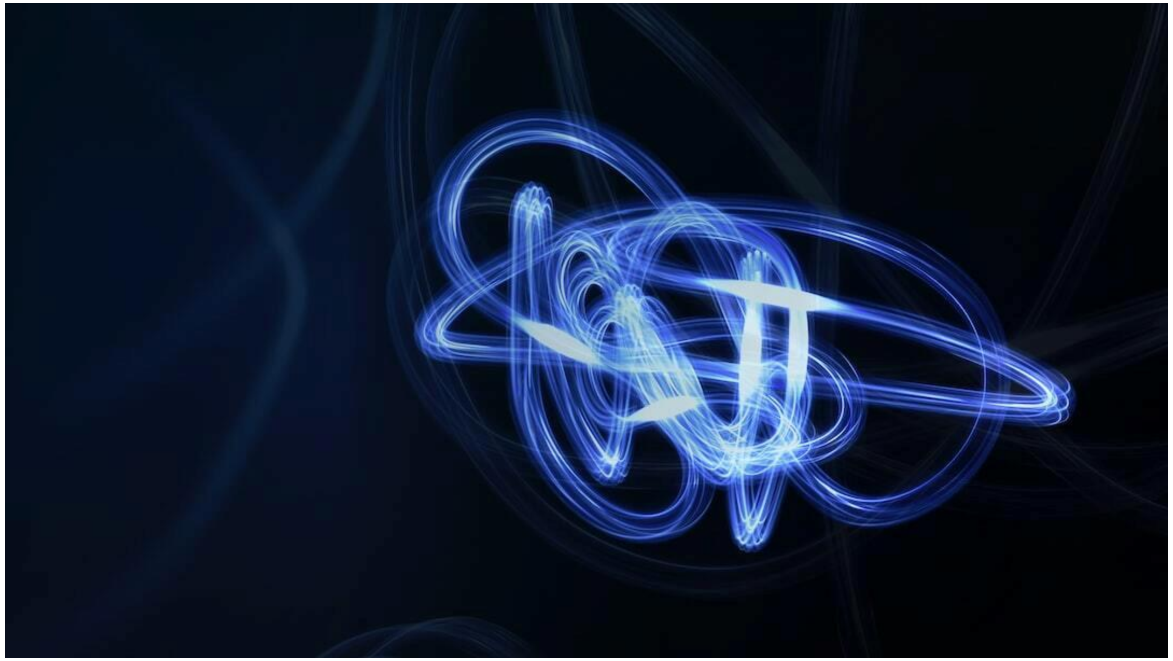


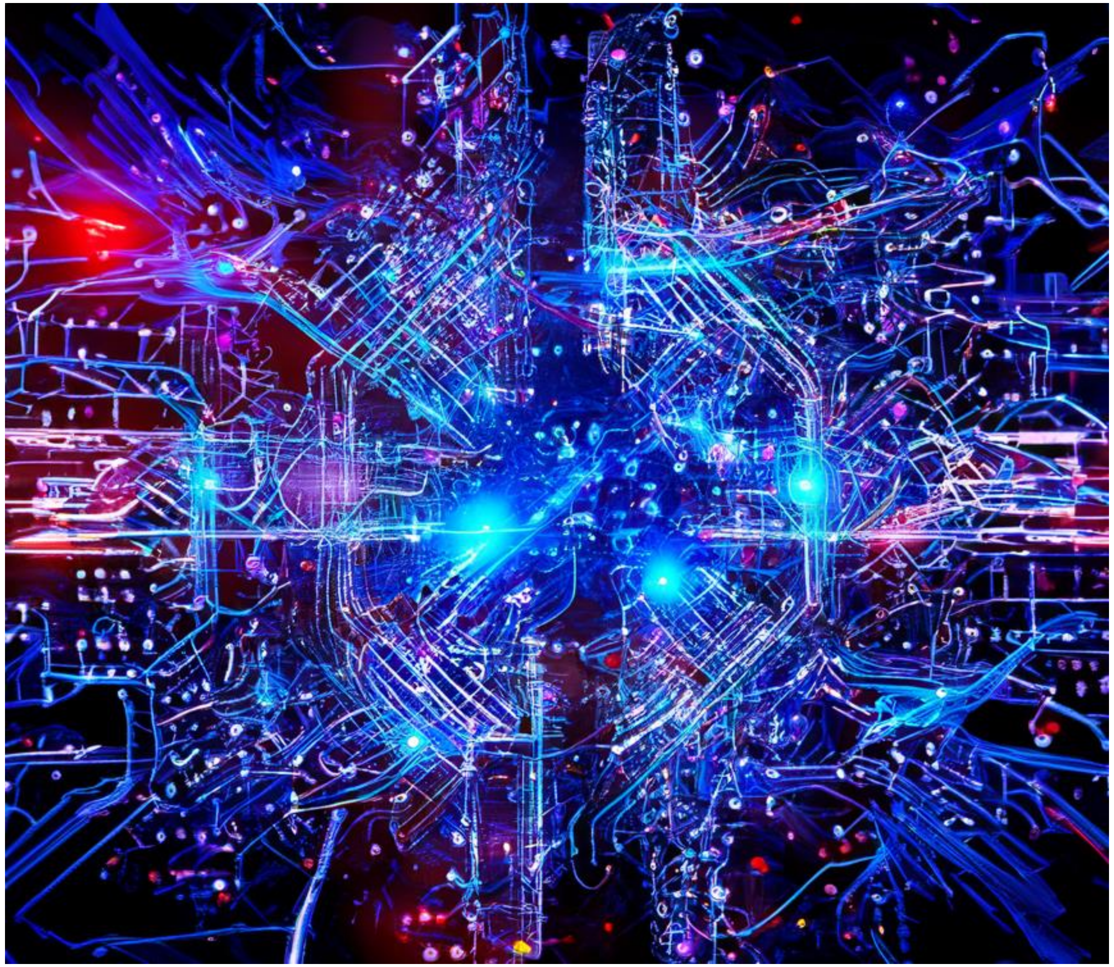
Photo by sourav sinha on Unsplash

Quantum Gates and Circuits

Quantum Gates: Operate on qubits, altering their states through operations like Pauli-X, Hadamard, and CNOT.

Quantum Circuits: Sequences of quantum gates combined to perform complex computations.

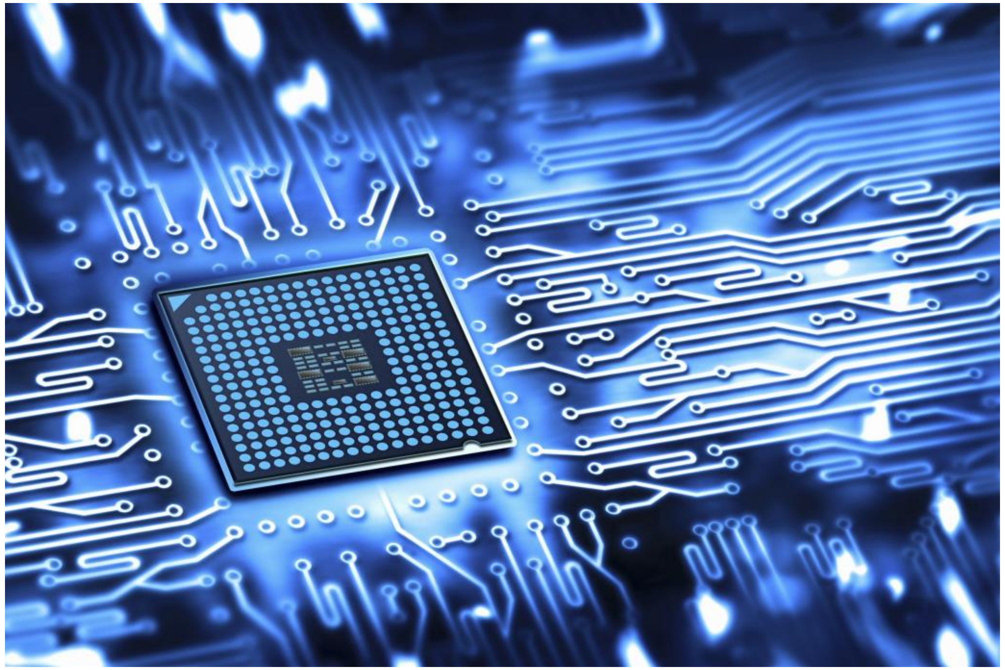
Example: Quantum circuits can solve specific problems much faster than classical algorithms.



Adobe Photoshop generated – Prompt:“Quantum Circuits”

Classical and Quantum Computing Differences

Classical Computing: Uses bits as basic units of information, processing sequentially.



Quantum Computing: Uses qubits, leveraging superposition and entanglement for parallel processing.

Performance: Quantum computing can solve certain problems exponentially faster than classical computing.

Milestones in Quantum Computing Development

1980s: Theoretical Foundations: Richard Feynman and David Deutsch propose quantum computing principles.

1994: Shor’s Algorithm: Peter Shor develops an algorithm for integer factorization, showing potential of quantum computing.

1998: First Quantum Computer: Isaac Chuang (Los Alamos Labs) + others from UC Berkeley and MIT

2019: Quantum Supremacy: Google claims quantum supremacy with their Sycamore processor.

2024: Building Quantum Computers with new techniques

- https://phys.org/news/2024-06-technique-quantum-future.html
- https://www.earth.com/news/building-quantum-computers-just-got-easier-with-new-technique/

Practical Applications

Quantum Computing in Healthcare (Drug Discovery)

Drug Discovery

- Quantum computing can simulate molecular interactions, speeding up drug discovery.

Personalized Medicine

- Enhances the ability to analyze genetic information for personalized treatment plans.

Clinical Trials

- Optimizes the design and analysis of clinical trials for better outcomes.

Quantum Computing in Cryptography

Quantum Key Distribution (QKD)

- Provides theoretically secure communication channels leveraging quantum principles.

Future of Cryptography

- The development of post-quantum cryptography to secure data against quantum attacks.

Encryption Breaking

- Quantum computers can potentially break classical encryption schemes, necessitating quantum-safe cryptography.

Quantum Computing in Finance (Optimization)

Portfolio Optimization

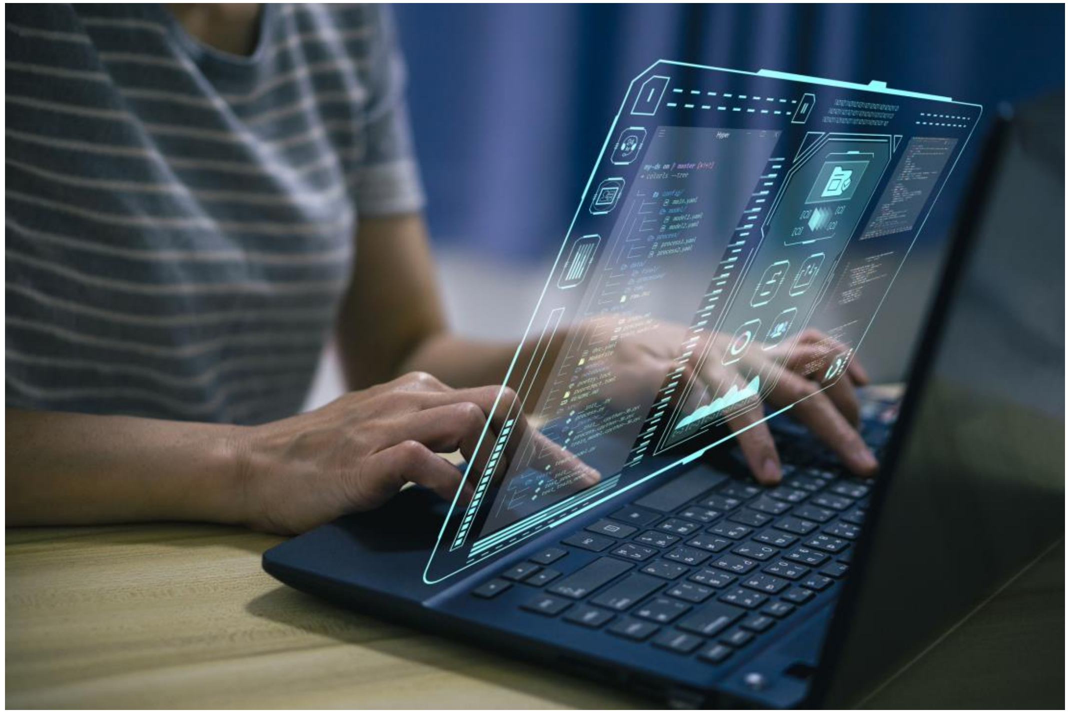
- Quantum algorithms optimize investment portfolios for better returns.

Risk Analysis

- Improves risk management by analyzing vast amounts of data quickly.

Fraud Detection

- Enhances the ability to detect and prevent financial fraud with greater accuracy.



Quantum Computing in Logistics (Supply Chain Management)

Route Optimization

- Quantum algorithms can optimize delivery routes, reducing time and cost.

Inventory Management

- Enhances accuracy in predicting inventory needs, reducing waste.

Supply Chain Coordination

- Improves synchronization across the supply chain, increasing efficiency.

Licensed through: Getty Images

Quantum Fears?

Quantum Sized Fear

Security Threats

Breaking existing encryption, putting sensitive data at risk.

Job Displacement

Automation and advanced problem-solving capabilities may lead to job losses in certain sectors.

Ethical Issues

Concerns about its misuse and the digital divide.

Privacy Concerns

Processing vast amounts of data quickly may lead to increased surveillance and privacy invasions.

Economic Disruption

Disruption to existing business models and new competitive dynamics.

Quantum Computing Will Expose Our Secrets!!!

The headlines:

“Modern Encryption Methods Will Be Rendered Useless” – Forbes[1]

“U.S. and China race to shield secrets from quantum computers” – Reuters[2]

“Today's impenetrable cryptographic codes could soon be history.” – International Monetary Fund[3]

“Bad actors and nation-states are deploying “harvest now, decrypt later” strategies that target sensitive data that will still be valuable when they are finally able to access it (also called ‘long-lived data’).” – Wall Street Journal[4]

Security Threats

Breaking existing encryption, putting sensitive data at risk.

[1] https://www.forbes.com/sites/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/

[2] https://www.reuters.com/investigates/special-report/us-china-tech-quantum/

[3] https://www.imf.org/en/Publications/fandd/issues/2021/09/quantum-computings-possibilitiesand-perils-Deodoro

[4] https://partners.wsj.com/entrust/the-post-quantum-cybersecurity-threat/prepare-your-organization-and-your-data-for-quantum-computers/

Security Risks: Breaking Classical Encryption

Everyone is looking at this first!

Encryption Vulnerability

- Quantum computers could potentially break widely used encryption methods, such as RSA and ECC.

Data Security

- Sensitive information currently protected by classical encryption could be at risk.

Post-Quantum Cryptography

- Development of quantum-resistant encryption methods is essential for future security.

Literature-Reported Estimates of Quantum Resilience

For Current Cryptosystems, Under Various assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM[c]	Symmetric encryption	128	128	Grover's algorithm	2953	4.61×10^{6}	2.61×10^{12} years	
		192	192		4449	1.68×10^{7}	1.97×10^{22} years	
		256	256		6681	3.36×10^{7}	2.29×10^{32} years	
RSA[d]	Asymmetric encryption	1024	80	Shor's algorithm	2050	8.05×10^{6}	3.58 hours	Move to NIST-selected PQC algorithm when available
		2048	112		4098	8.56×10^{6}	28.63 hours	
		4096	128		8194	1.12×10^{7}	229 hours	
ECC Discrete-log problem[e-g]	Asymmetric encryption	256	128	Shor's algorithm	2330	8.56×10^{6}	10.5 hours	Move to NIST-selected PQC algorithm when available
		384	192		3484	9.05×10^{6}	37.67 hours	
		521	256		4719	1.13×10^{6}	55 hours	
SHA256[h]	Bitcoin mining	N/A	72	Grover's algorithm	2403	2.23×10^{6}	1.8×10^{4} years	
PBKDF2 with 10,000 iterations[i]	Password hashing	N/A	66	Grover's algorithm	2403	2.23×10^{6}	2.3×10^{7} years	Move away from password-based authentication

"4 Quantum Computing's Implications for Cryptography." National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. doi: 10.17226/25196. National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

https://nap.nationalacademies.org/read/25196/chapter/6#98

EXPLORE

The Secret Reality

Personal data: How many are on social media platforms?

Business data:

- What % of today’s data will need protected/encrypted in X years?

Use quantum resistant encryption – CRYSTALS, FALCON, SPHINCS+[1]

“‘I think companies will forget the hype and implement the weakest thing that comes out of NIST until they are suddenly reminded of the problem in 30 years,’ Vadim Lyubashevsky, a cryptographer at IBM who’s working on post-quantum cryptographic algorithms with NIST, told MIT Technology Review last year.” – MIT Technology Review[2]

Security Threats

Breaking existing encryption, putting sensitive data at risk.

[1] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[2] https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/

Jobs Losses due to Quantum Computing

The headlines:

“The increased processing power and efficiency of quantum computers could automate many jobs currently performed by humans, leading to potential job displacement.” – Illinois Law Review[1]

“The unemployment threat posed by automation increases when considering that employers are incentivized to automate their workforce.” – Illinois Law Review[1]

Job Displacement

Automation and advanced problem-solving capabilities may lead to job losses in certain sectors.

[1] https://illinoislawreview.org/online/they-took-our-jobs/

Keeping the Lights On…

"In 1900, 41 percent of the US workforce was employed in agriculture; by 2000, that share had fallen to 2 percent (Autor 2014), mostly due to a wide range of technologies including automated machinery." – MIT[1]

The June 2024 Unemployment rate was 4.1% – Federal Reserve Bank of St. Louis[2]

"The basic fact is that technology eliminates jobs, not work." – Harvard Business Review[3]

"Factory workers that manually assembled cars might find themselves displaced by robots, but these robots need to be built and serviced by people. If quantum computers make certain jobs obsolete, they open other opportunities." – Scientific Computing[4]

20 jobs that didn't exist 20 years ago

- AI Engineer
- Driverless car engineer
- Data scientist
- Cloud architect
- Automation engineer
- User experience designer
- Mobile app developer
- Developer evangelist
- Social media manager
- Digital strategist
- SEO analyst
- Community manager
- Head of culture
- Podcast producer
- Drone pilot
- Motion graphic designer
- Telemedicine physician or psychologist
- Genetic counselor
- Sustainability manager
- FinTech analyst

https://blog.intostudy.com/uncategorized/20-jobs-that-didnt-exist-20-years-ago/

[1] https://economics.mit.edu/research/publications/why-are-there-still-so-many-jobs-history-and-future-workplace-automation

[2] https://fred.stlouisfed.org/series/UNRATE

[3] https://hbr.org/2018/01/the-question-with-ai-isnt-whether-well-lose-our-jobs-its-how-much-well-get-paid

[4] https://www.scientific-computing.com/article/quantum-computing-ethics

What to Study

In the 1900's

- Common sense said "be a farmer"
- Uncommon sense said "be an electrical engineer"

The fastest growing occupations of 2022 are:[1]

- Wind turbine service technicians
- Nurse practitioners
- Data scientists
- Statisticians
- Information security analysts

What do you do with quantum results?

"McKinsey predicts that by 2025, fewer than half of quantum jobs will be filled, which is a major barrier to adoption." – MIT Sloan[2]

Fastest Declining Occupations, 2022[1]

- Word processors and typists
- Watch and clock repairers
- Roof bolters, mining
- Cutters and trimmers, hand
- Telephone operators
- Data entry keyers
- Switchboard operators, including answering service

Job Displacement

Automation and advanced problem-solving capabilities may lead to job losses in certain sectors.

[1] https://www.bls.gov/emp/tables/emp-by-detailed-occupation.htm

[2] https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now

Life or Death Decisions…

The headlines:

“Under what conditions can we trust the outputs of a (quantum) black box model?

What are the appropriate benchmarks for performance?

What do we do if the system appears to be broken or is acting very strangely?

Do we acquiesce to the inscrutable outputs of the machine that has proven reliable previously?

Or do we eschew those outputs in favor of our comparatively limited but intelligible human reasoning?” – Harvard Business Review[1]

Ethical Issues

Concerns about its misuse and the digital divide.

[1] https://hbr.org/2023/05/how-to-avoid-the-ethical-nightmares-of-emerging-technology

Ethical and Societal Implications

Employment Impact

- Disruption may lead to job displacement.
- Likely to create new opportunities.

Digital Divide

- Access to quantum technology may widen the gap between different socioeconomic groups and first/third world countries.
- Potential creative ways to solve social issues

Privacy Concerns

- Potential to break current encryption raises significant privacy issues.
- Ability to leverage quantum encryption

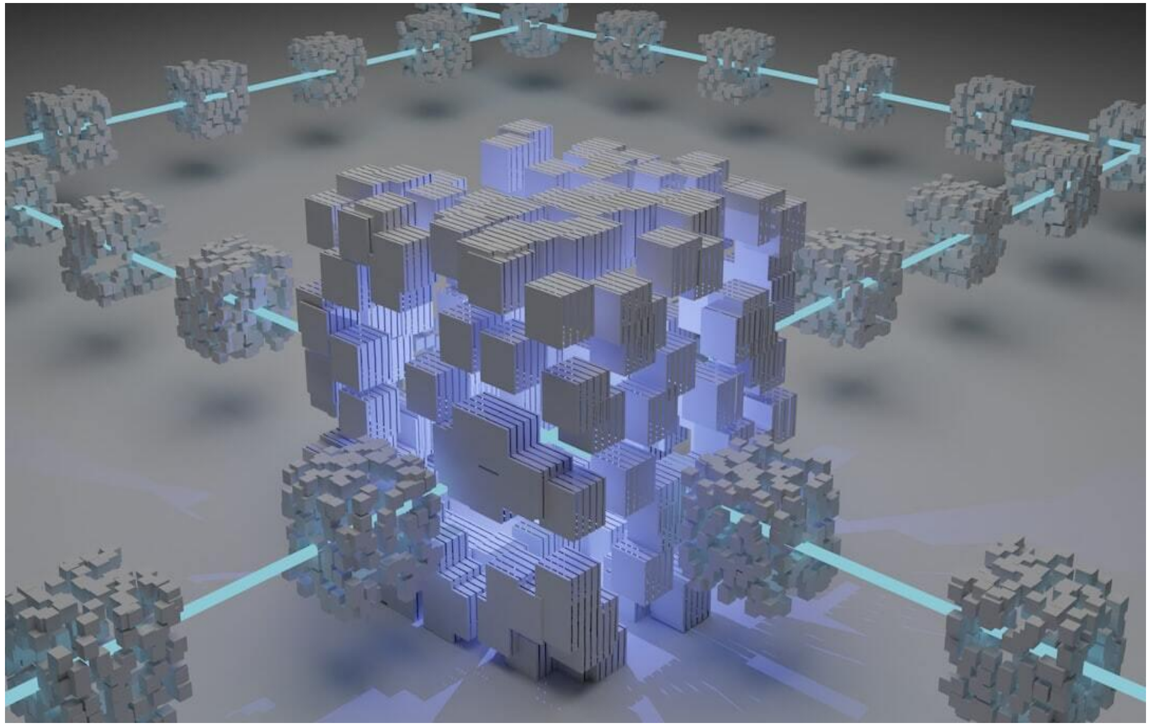


Photo by Shubham Dhage on Unsplash

Irrational Humans

“…Predicting users’ next actions.” – The Quantum Record[1]

“…Explain human behavior in a more consistent way. ...[the idea of] artificial quantum intelligence (AQI)” – Phys.org[2]

“What changes in the world, once databases know enough about you to guess your beliefs, your motives, your objectives, your ideals, to enable every message you see and hear to appeal directly to you?” – ZDNET.com[3]

“If you came up with a 'quantum' way of computing the results of the forecast [for an election], the results would be the same -- you just would get them faster. ” – ZDNET.com[3]

Ethical Issues

Concerns about its misuse and the digital divide.

[1] https://thequantumrecord.com/philosophy-of-technology/quantum-ethics-plan-for-human-future/

[2] https://phys.org/news/2024-01-quantum-physics-key-secrets-human.html

[3] https://www.zdnet.com/article/could-quantum-computers-fix-political-polls/

Our Thoughts Aren’t Even Our Own

The headlines:

“A team of researchers in China has unveiled a technique that—theoretically—could crack the most common methods used to ensure digital privacy[…]” – Scientific America[1]

“[…quantum computing] raises questions about the safeguards that might be appropriate to put in place in order to comply with laws like the California Consumer Protection Act (CCPA) and the New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act).” – Bloomberg Law [2]

Privacy Concerns

Processing vast amounts of data quickly may lead to increased surveillance and privacy invasions.

[1] https://www.scientificamerican.com/article/are-quantum-computers-about-to-break-online-privacy/

[2] https://www.bloomberglaw.com/external/document/X24KPL64000000/international-data-privacy-compliance-professional-perspective-t

Regulatory and Policy Issues

Data Protection

- Ensuring robust data protection frameworks to address quantum computing threats.

Regulation

- Harmonizing international regulations on quantum technology use and development.
- Addressing privacy laws to keep up to date with modern advances

Funding and Support

- Government policies to support quantum research and address associated risks.

A New View of the World

GDPR:

- “The organisation will fall short of its requirement to take appropriate security measures to protect personal data against ‘unauthorised processing’…” – Society for Computers & Law[1]
- “…GDPR protects data subjects against automated decision making (such as profiling), it will become a tricky issue to measure the compliance of supercomputers…” – Society for Computers & Law[1]
- “Essentially, personal data must be processed in a manner that is lawful, compliant and transparent. This due diligence principle is the bedrock of the GDPR and forms the foundation for the remaining data protection requirements.” – Society for Computers & Law[1]

Privacy Concerns

Processing vast amounts of data quickly may lead to increased surveillance and privacy invasions.

[1] https://bytes.scl.org/a-qubit-evolution/

Quantum Computing Will Disrupt Economies!!!

The headlines:

“Quantum Computing Could Deliver ‘Next Global Shock’: WEF” – IOT World Today[1]

“Why Quantum Computing Is Even More Dangerous Than Artificial Intelligence” – ForeignPolicy.com[2]

“Can we build a safe and inclusive 'quantum economy’?” – World Economic Forum[3]

“The quantum crisis threatens patient health, the large and lucrative healthcare industry, society, and even a country’s national security.” – qnulabs.com[4]

Economic Disruption

Disruption to existing business models and new competitive dynamics.

[1] https://www.iotworldtoday.com/quantum/quantum-computing-could-deliver-next-global-shock-wef2

[2] https://foreignpolicy.com/2022/08/21/quantum-computing-artificial-intelligence-ai-technology-regulation/

[3] https://www.weforum.org/agenda/2024/02/quantum-economy-blueprint-world-economic-forum/

[4] https://www.qnulabs.com/quantum-security-health-industry/

Economic and Investment Risks

High Costs

- Developing and maintaining quantum computers requires significant investment.

Uncertain ROI

- Uncertainty about the time frame for practical, large-scale applications impacts return on investment.

Market Volatility

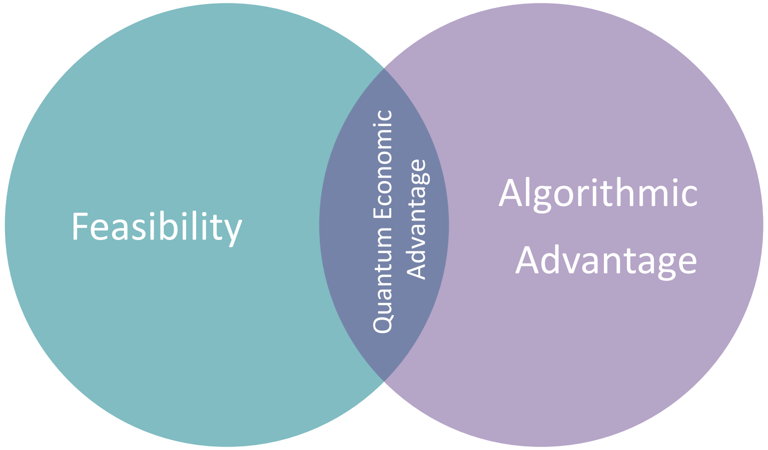
- Rapid advancements and competition can lead to market volatility and investment risks.

Quantum Economic Advantage

MIT Sloan:[1]

To determine the quantum economic advantage, business and technology leaders will have to consider two conditions:

- **Feasibility**, meaning whether a quantum computer exists that is sufficiently powerful to solve a particular problem.
- **Algorithmic advantage**, meaning that a quantum computer would be faster at completing a particular task compared with a comparably priced classical computer.



[1] https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now

Economic Disruption

Disruption to existing business models and new competitive dynamics.

EXPLORE

Visions From Quantum Foam

A Look Into the Future

“Quantum computing is not a replacement for classical computing, nor is it a standalone compute solution” – Dell[1]

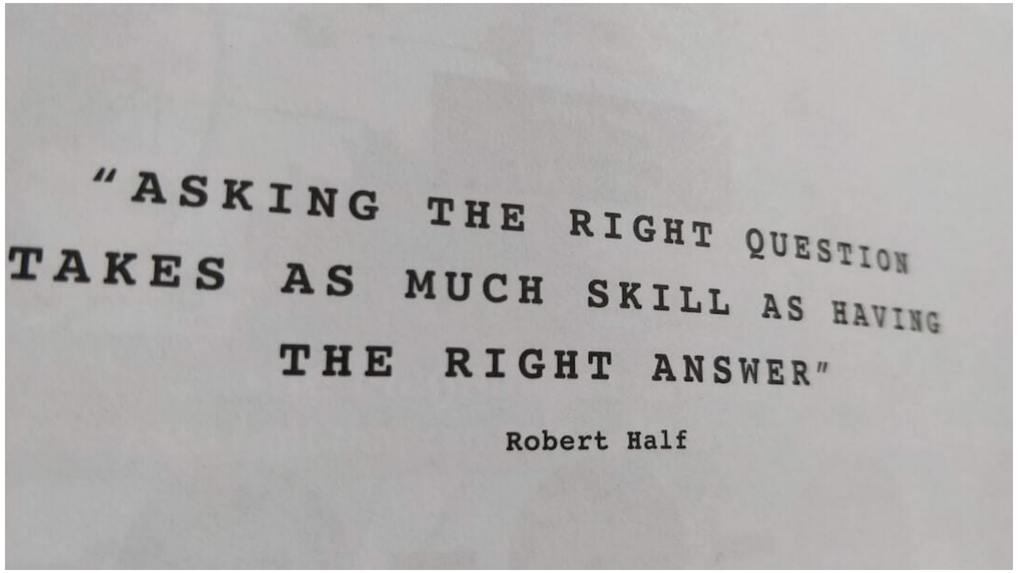
"Broadcom is thrilled to partner with Caltech to launch this critical R&D initiative on quantum computing. As a world-class leader in science and engineering research, Caltech has a long and rich history of technology innovation," says Hock Tan, President and CEO of Broadcom.[2] (see also: https://youtu.be/SPPYa2Otzpo?si=o9CK6GRZL8nlHi1f&t=1464)

[1] https://www.delltechnologies.com/asset/en-us/products/ready-solutions/industry-market/hyperion-quantum-computing-paper.pdf

[2] https://www.caltech.edu/about/news/caltech-and-broadcom-announce-quantum-research-and-development-partnership

What are Your Thoughts?

“Right now, we have small, general-purpose quantum computers that can basically do anything you ask them to, if you ask nicely. Then we have large, special-purpose quantum computers that can solve specific problems better than classical computers can. What we don't have is a large, general-purpose quantum computer of the sort that would be needed to break codes, strike fear in the heart of the National Security Agency and other three-letter agencies. Which is probably a good thing.” – Seth Lloyd[1]



“ASKING THE RIGHT QUESTION TAKES AS MUCH SKILL AS HAVING THE RIGHT ANSWER”

Robert Half

Photo by David Carboni on Unsplash

[1] http://www.notable-quotes.com/l/lloyd_seth.html

EXPLORE

Please take your survey.

EXPLORE

Stay Connected

Let’s continue the conversation

Follow us @vcdx001 and @wonder_nerd

EXPLORE

Thank you