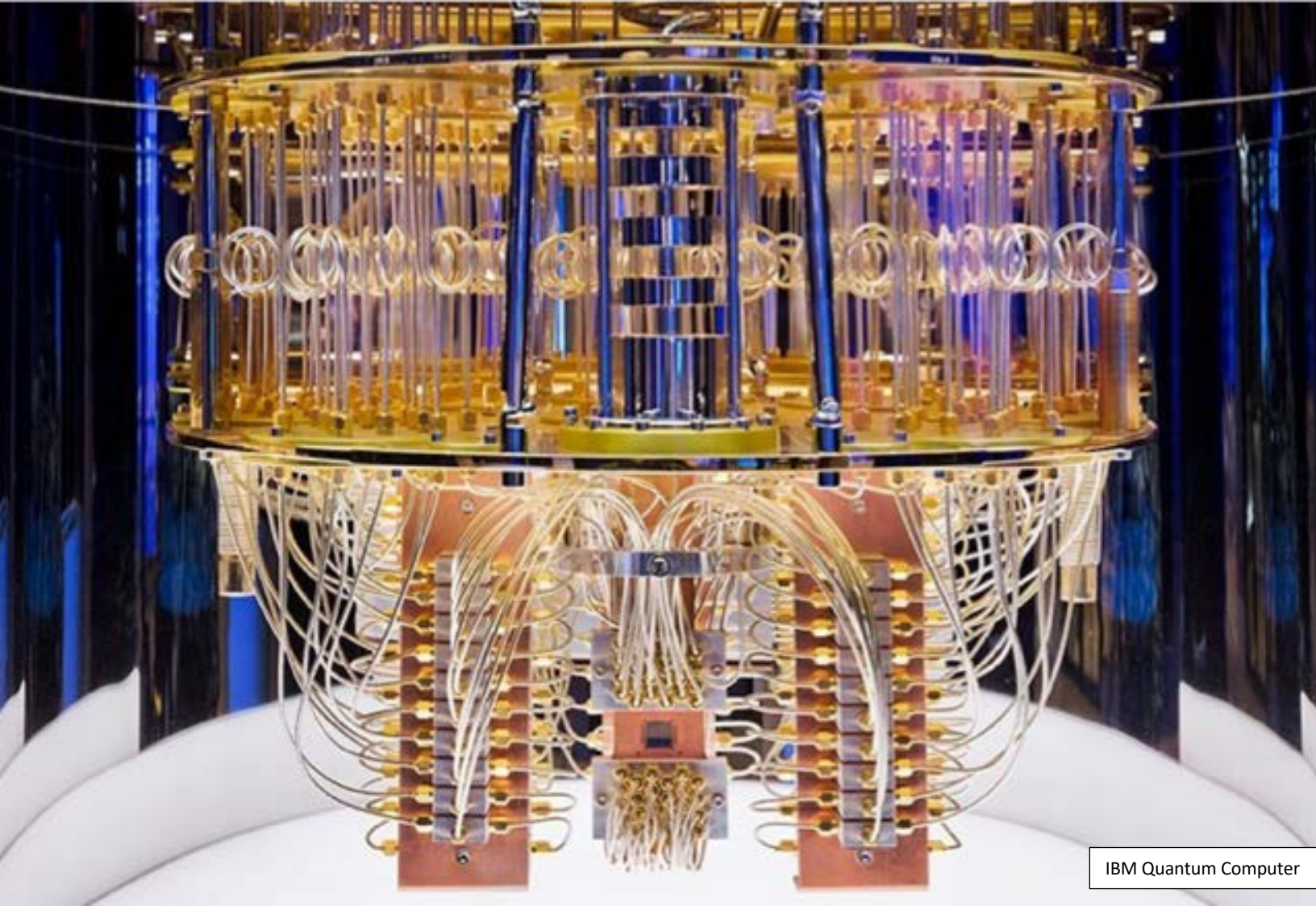


IBM Quantum Computer

Quantum Technologies

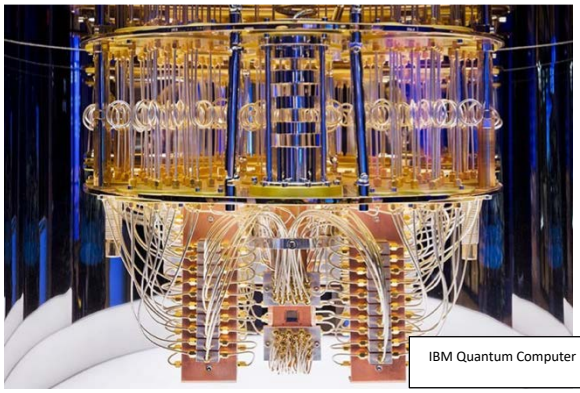
Author: Steve Blank

Stanford | Gordian Knot Center for National Security Innovation

https://gordianknot.stanford.edu

The Quantum Technology Ecosystem – Explained

If you think you understand quantum mechanics,
you don't understand quantum mechanics
Richard Feynman

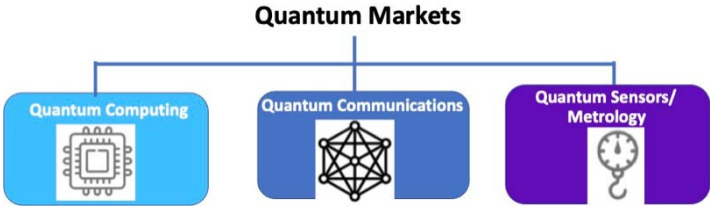

IBM Quantum Computer

Tens of billions of public and private capital are being invested in Quantum technologies. Countries across the world have realized that quantum technologies can be a major disruptor of existing businesses and change the balance of military power. So much so, that they have collectively invested ~$24 billion in in quantum research and applications.

At the same time, a week doesn't go by without another story about a quantum technology milestone or another quantum company getting funded. Quantum has moved out of the lab and is now the focus of commercial companies and investors. In 2021 venture capital funds invested over $2 billion in 90+ Quantum technology companies. Over a $1 billion of it going to Quantum computing companies. In the last six months quantum computing companies IonQ, D-Wave and Rigetti went public at valuations close to a billion and half. Pretty amazing for computers that won't be any better than existing systems for at least another decade – or more. So why the excitement about quantum?

The Quantum Market Opportunity

While most of the IPOs have been in Quantum Computing, Quantum technologies are used in three very different and distinct markets: Quantum *Computing*, Quantum *Communications* and Quantum *Sensing and Metrology*.



All of three of these markets have the *potential* for being disruptive. In time Quantum *computing* could obsolete existing cryptography systems, but viable commercial applications are still speculative. Quantum *communications* could allow secure networking but are not a viable near-term business. Quantum *sensors* could create new types of medical devices, as well as new classes of military applications, but are still far from a scalable business.

It's a pretty safe bet that 1) the largest commercial applications of quantum technologies won't be the ones these companies currently think they're going to be, and 2) defense applications using quantum technologies will come first. 3) if and when they do show up they'll destroy existing businesses and create new ones.

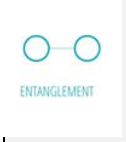
We'll describe each of these market segments in detail. But first a description of some quantum concepts.

Key Quantum Concepts

Skip this section if all you want to know is that 1) quantum works, 2) yes, it is magic.

Quantum - The word "Quantum" refers to quantum mechanics which explains the behavior and properties of atomic or subatomic particles, such as electrons, neutrinos, and photons.

Superposition – quantum particles exist in many possible states at the same time. So a particle is described as a "superposition" of all those possible states. They fluctuate until observed and measured. Superposition underpins a number of potential quantum computing applications.



Entanglement – is what Einstein called "spooky action at a distance." Two or more quantum objects can be linked so that measurement of one dictates the outcomes for the other, regardless of how far apart they are. Entanglement underpins a number of potential quantum communications applications.

Observation – Superposition and entanglement only exist as long as quantum particles are not observed or measured. If you observe the quantum state you can get information, but it results in the collapse of the quantum system.

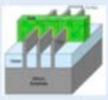
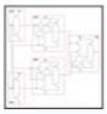
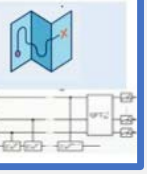
Qubit – is short for a quantum bit. It is a quantum computing element that leverages the principle of superposition to encode information via

one of four methods: spin, trapped atoms and ions, photons, or superconducting circuits.

Quantum Computers - Background

Quantum computers are a really cool idea. They harness the unique behavior of quantum physics—such as superposition, entanglement, and quantum interference—and apply it to computing.

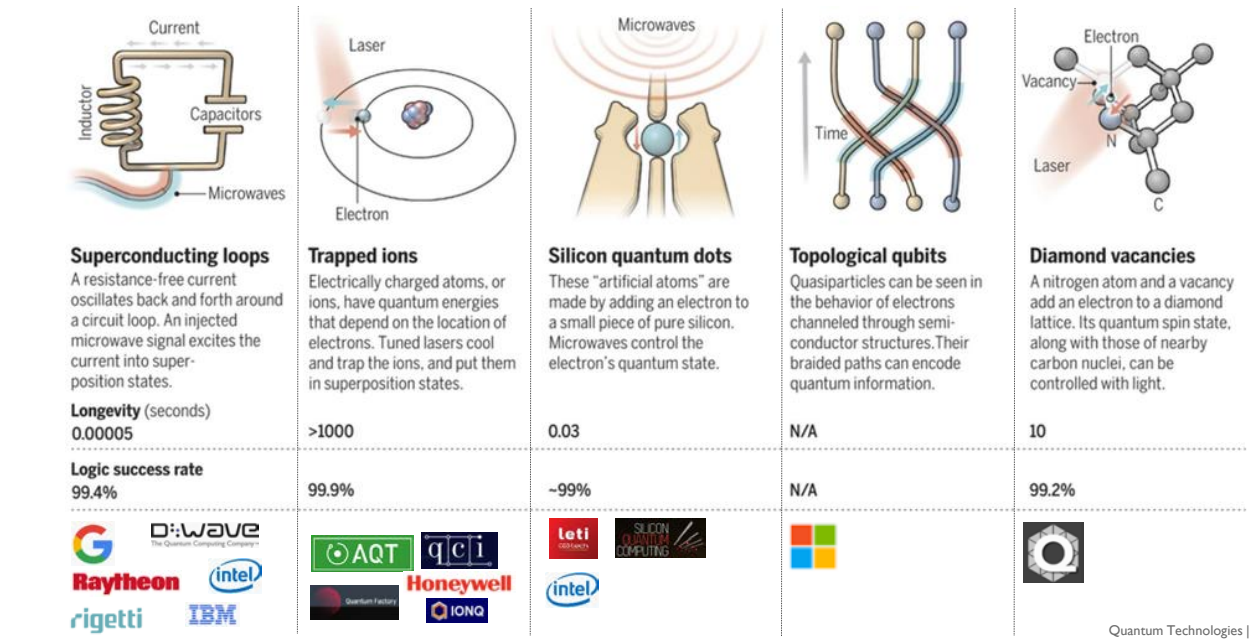
In a classical computer transistors can represent two states - either a 0 or 1. Instead of transistors Quantum computers use quantum bits (called *qubits.) Qubits* exist in *superposition* - both in 0 and 1 state simultaneously.

Classical Computers		Quantum Computers	
Calculates with transistors which can represent *either* 0 or 1		Calculates with Qubits, which can represent 0 and 1 *simultaneously*	
Uses transistors to create these logical switches		Uses either trapped ions, superconducting loops, quantum dots, diamond vacancies to create Qubits	
Multiple transistors (~2-14) make up basic logic gates		Multiple Qubits make up a logical Qubit (9-100's?)	
Compute power scales in a 1-to-1 relationship with the number of transistors and clock speed		Compute power increases exponentially in proportion to the number of logical Qubits	
Low error rates and operate at room temperature		High error rates and need to be ultracold	
Used for general purpose computing		Used for optimization and factoring. A sufficient number of Qubits = *Cryptographically Relevant Quantum Computer*	

Classic computers use transistors as the physical building blocks of logic. In quantum computers they may use trapped ions, superconducting loops, quantum dots or vacancies in a diamond. The jury is still out.

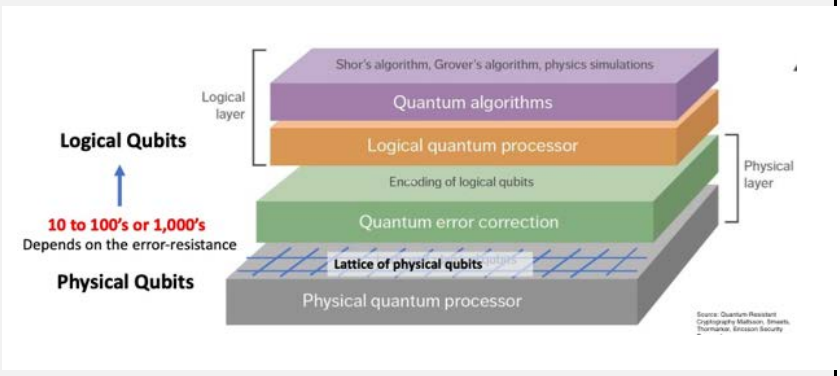
In a classic computer 2-14 transistors make up the seven basic logic gates (AND, OR, NAND, etc.) In a quantum computer building a single logical Qubit require a

minimum of 9 but more likely 100's or thousands of physical Qubits (to make up for error correction, stability, decoherence and fault tolerance.)



In a classical computer compute-power increases linearly with the number of transistors and clock speed. In a Quantum computer compute-power increases exponentially with the addition of each logical qubit.

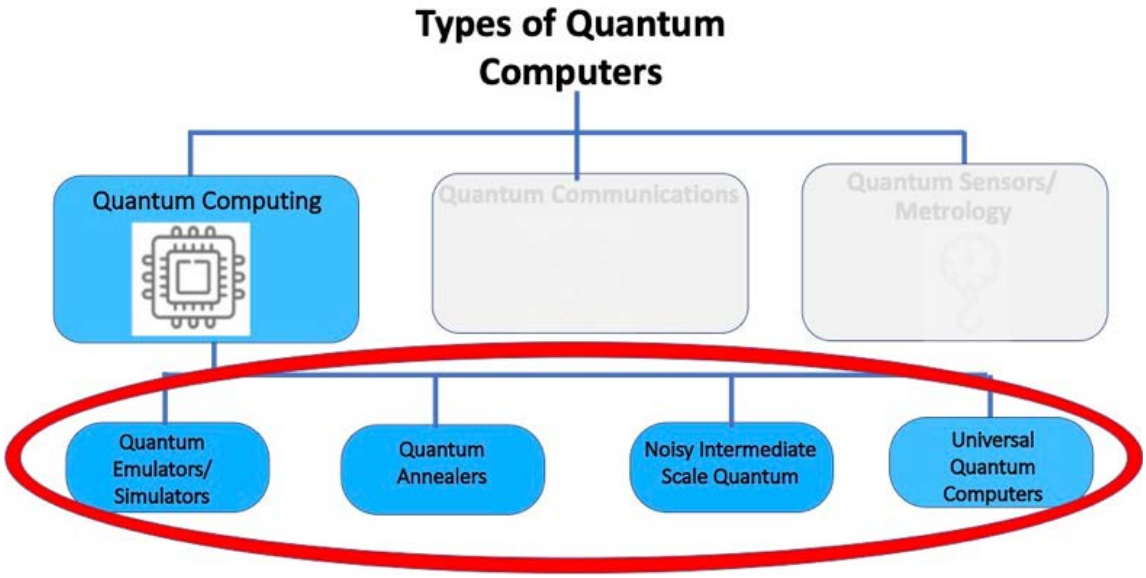
But qubits have high error rates and need to be ultracold. In contrast classical computers have very low error rates and operate at room temperature.



Finally, classical computers are great for general purpose computing. But quantum computers can theoretically solve *some* complex algorithms/problems exponentially faster than a classical computer. And with a sufficient number of logical Qubits they can become a *Cryptographically Relevant Quantum Computer* (CRQC). And this is where Quantum computers become very interesting and relevant for both commercial and national security. (More below.)

Types of Quantum Computers

Quantum computers could *potentially* do things at speeds current computers cannot. Think of the difference of how fast you can count on your fingers versus how fast today's computers can count. That's the same order of magnitude speed-up a quantum computer could have over today's computers for certain applications.



Quantum computers fall into four categories:

1. Quantum Emulator/Simulator
2. Quantum Annealer
3. NISQ – Noisy Intermediate Scale Quantum
4. Universal Quantum Computer – which can be a *Cryptographically Relevant Quantum Computer (CRQC)*

When you remove all the marketing hype, the only type that matters is #4 - a Universal Quantum Computer. And we're at least a decade or more away from having those.

Quantum Emulator/Simulator

These are classical computers that you can buy today that simulate quantum algorithms. They make it easy to test and debug a quantum algorithm that someday may be able to run on a Universal Quantum Computer. Since they don't use any quantum hardware they are no faster than standard computers.

	Quantum Emulators	Quantum Annealer	Noisy Intermediate Scale Quantum – (NISQ)	Universal Quantum - Cryptographically Relevant Quantum Computer (CRQC)
Function	Classical computer simulating quantum algorithms. No faster than existing computers	Focus on Optimization problems. Not building logical gates or universal computers	Currently a few noisy Qubits. Training wheels for future systems	The ultimate goal
Number of Physical Qubits	**0**	**0 (or 5,000)** D-Wave 5000-qubit system – not gate based.	**50-100**	**50-100** Possibly millions needed
Companies	TOSHIBA, FUJITSU, HITACHI Inspire the Next, Atos, Microsoft	D-Wave	IBM, Google, rigetti, Raytheon	Microsoft, 阿里云, Honeywell, PASQAL, IONQ, ANAMETRIC, intel

Quantum Annealer is a special purpose quantum computer designed to only run combinatorial optimization problems, *not* general-purpose computing, or cryptography problems. D-Wave has defined and owned this space. While they have more physical Qubits than any other current system they are not organized as gate-based logical qubits. Currently this is a nascent commercial technology in search of a future viable market.

Noisy Intermediate-Scale Quantum (NISQ) computers. Think of these as *prototypes* of a Universal Quantum Computer – with several orders of magnitude fewer bits. (They currently have 50-100 qubits, limited gate depths, and short coherence times.) As they are short several orders of magnitude of Qubits, NISQ computers cannot perform any useful computation and are the training wheels for future universal quantum computers.

Universal Quantum Computers / Cryptographically Relevant Quantum Computers (CRQC)

This is the ultimate goal. If you could build a universal quantum computer with fault tolerance (i.e. millions of error corrected physical qubits resulting in thousands of logical Qubits), you could run quantum algorithms in cryptography,

search and optimization, quantum systems simulations, and linear equations solvers. (See here for a list of hundreds quantum algorithms.) These all would dramatically outperform classical computation. These special algorithms are what make quantum computers *potentially* valuable. For example, Grover's algorithm solves the problem for the unstructured search of data. However, while all of these algorithms *might* have commercial potential one day, no one has yet to come up with a use for them that would radically transform any business or military application. Except for one – and that one keeps people awake at night.

It's Shor's algorithm for integer factorization – an algorithm that underlies much of existing public cryptography systems.

The security of today's public key cryptography systems rests on the assumption that breaking into those with a thousand or more digits is practically impossible. It requires factoring into large prime numbers (e.g., RSA) or elliptic curve (e.g., ECDSA, ECDH) or finite fields (DSA) that can't be done with any type of classic computer regardless of how large. Shor's factorization algorithm can crack these codes if run on a Universal Quantum Computer. Uh-oh!

Impact of a Cryptographically Relevant Quantum Computer (CRQC)
Skip this section if you don't care about cryptography.

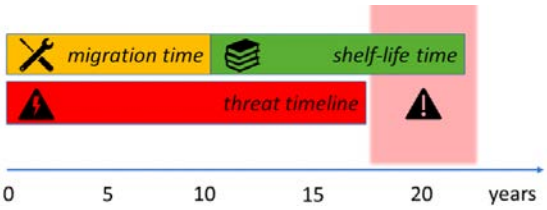
Not only would a Universal Quantum Computer running Shor's algorithm make today's public key algorithms (used for asymmetric key exchanges and digital signatures) useless, someone can implement a "harvest-now-and-decrypt-later attack" to record encrypted documents now with intent to decrypt them in the future. *That means everything you send encrypted today will be able to be read retrospectively*. Many applications - from ATMs to emails - would be vulnerable—unless we replace those algorithms with those that are "quantum-safe".

When Will Current Crypto Systems Be Vulnerable?
The good news is that we're nowhere near having any viable Cryptographically Relevant Quantum Computer, now or in the next few years.

However, you can estimate when this *will* happen by calculating how many logical Qubits are needed to run Shor's Algorithm and how long it will it take to break these crypto systems.

There are lots of people tracking these numbers (see here and here). Their estimate is that using 8,194 logical qubits using 22.27 million physical qubits, it would take a quantum computer 20 minutes to break RSA-2048. The best estimate is that this might be possible in 8 to 20 years.

Post-Quantum /Quantum-Resistant Codes
That means if you want to protect the content you're sending now, you need to migrate to new Post-Quantum /Quantum-Resistant Codes. But There are three things to consider in doing so:

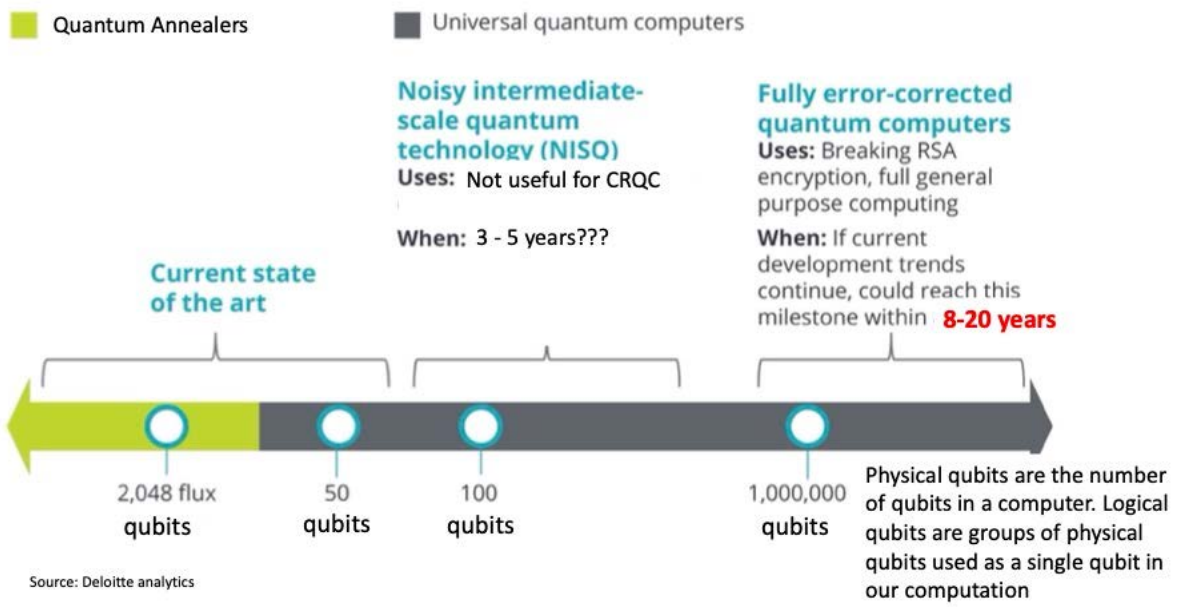


1. **shelf-life time**: the number of years the information must be protected by cyber-systems
2. **migration time**: the number of years needed to properly and safely migrate the system to a quantum-safe solution
3. **threat timeline**: the number of years before threat actors will be able to break the quantum-vulnerable systems

These new cryptographic systems would secure against both quantum and conventional computers and can interoperate with existing communication protocols and networks. The symmetric key algorithms of the Commercial National Security Algorithm (CNSA) Suite were selected to be secure for national security systems usage even if a CRQC is developed.

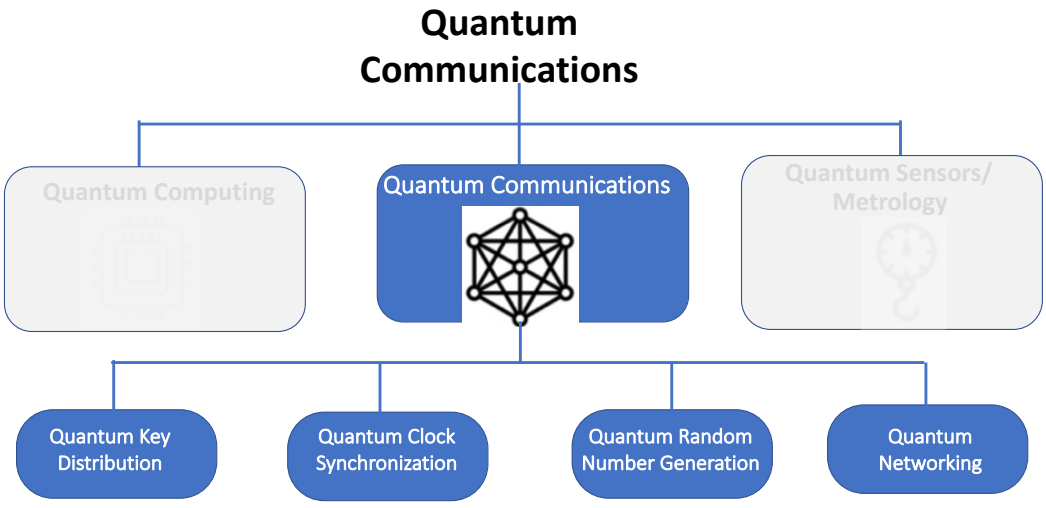
Cryptographic schemes that commercial industry believes are quantum-safe include lattice-based cryptography, hash trees, multivariate equations, and super-singular isogeny elliptic curves.

Estimates of when you can actually buy a fully error-corrected quantum computers vary from "never" to somewhere between 8 to 20 years from now.



Quantum Communication

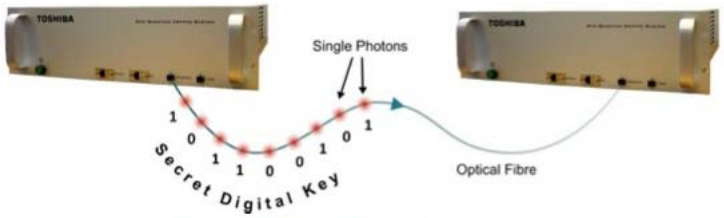
Quantum communications ≠ quantum computers. A quantum network's value comes from its ability to distribute entanglement. These communication devices manipulate the quantum properties of photons/particles of light to build Quantum Networks.
This market includes secure crypto key distribution, clock synchronization,



random number generation and networking of quantum military sensors, computers, and other systems.

Quantum Cryptography/Quantum Key Distribution

Quantum Cryptography/Quantum Key Distribution can distribute keys between authorized partners connected by a quantum channel and a classical authenticated channel. It can be implemented via fiber optics or free space transmission. China transmitted entangled photons (at one pair of entangled particles per second) over 1,200 km in a satellite link, using the Micius satellite.



Quantum Key Distribution Systems

The Good: it can detect the presence of an eavesdropper, a feature not provided in standard cryptography. The Bad: Quantum Key Distribution can't be implemented in software or as a service on a network and cannot be easily integrated into existing network equipment. It lacks flexibility for upgrades or security patches. Securing and validating Quantum Key Distribution is hard and it's only one part of a cryptographic system.

The view from the National Security Agency (NSA) is that quantum-resistant (or post-quantum) cryptography is a more cost effective and easily maintained solution than quantum key distribution. *NSA does not support the usage of QKD or QC to protect communications in National Security Systems*. (See here.) They do not anticipate certifying or approving any Quantum Cryptography/Quantum Key Distribution security products for usage by National Security System customers unless these limitations are overcome. However, if you're a commercial company these systems may be worth exploring.

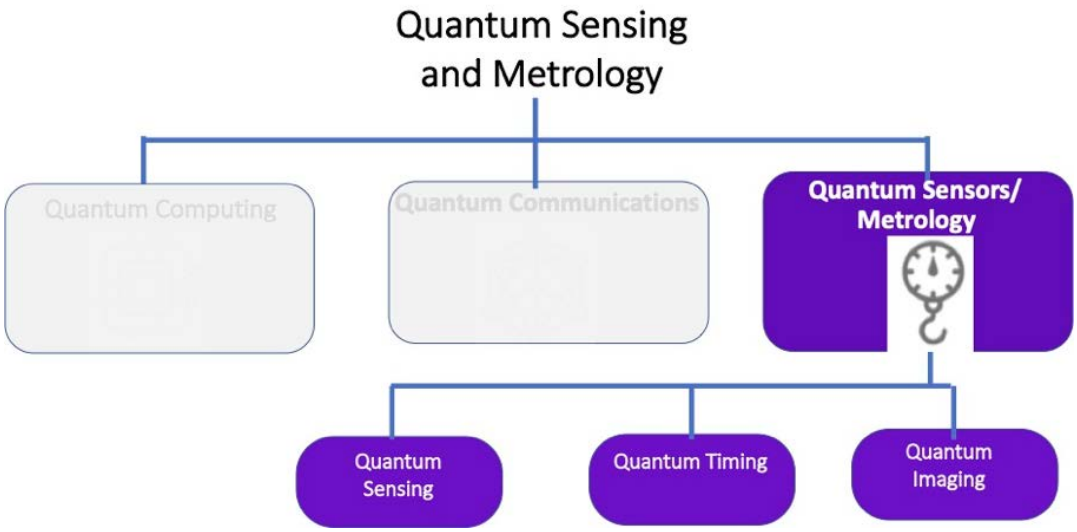
Quantum Random Number Generators (GRGs)

Commercial Quantum Random Number Generators that use quantum effects (entanglement) to generate nondeterministic randomness are available today. (Government agencies can already make quality random numbers and don't need these devices.)

Random number generators will remain secure even when a Cryptographically Relevant Quantum Computer is built.

Quantum Sensing and Metrology

Quantum sensors ≠ Quantum computers. This segment consists of Quantum *Sensing* (quantum magnetometers, gravimeters, ...), Quantum *Timing* (precise time measurement and distribution), and Quantum *Imaging* (quantum radar, low-SNR imaging, ...)



Each of these areas can create entirely new commercial products or entire new industries e.g. new classes of medical devices and military systems, e.g. anti-submarine warfare, detecting stealth aircraft, finding hidden tunnels and weapons of mass destruction. Some of these are achievable in the near term.

Quantum Timing

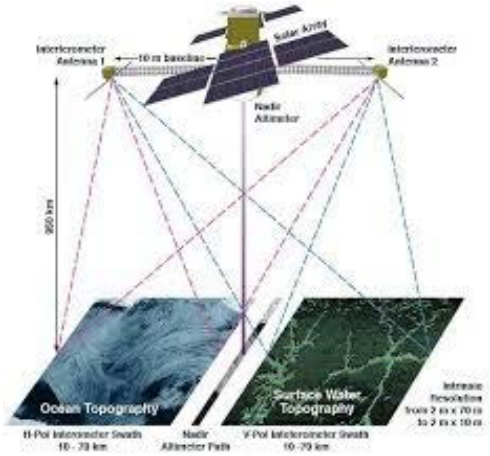
First-generation quantum timing devices already exist as microwave atomic clocks. They are used in GPS satellites to triangulate accurate positioning. The Internet and computer networks use network time servers and the NTP protocol to receive the atomic clock time from either the GPS system or a radio transmission.

The next generation of quantum clocks are even more accurate and use laser-cooled single ions confined together in an electromagnetic ion trap. This increased accuracy is not only important for scientists attempting to measure dark matter and gravitational waves, but miniaturized/ more accurate atomic clocks will allow precision navigation in GPS- degraded/denied areas, e.g. in commercial and military aircraft, in tunnels and caves, etc.

Quantum Imaging

Quantum imaging is one of the most interesting and near-term applications. First generation magnetometers such as superconducting quantum interference devices (SQUIDs) already exist. New quantum sensor types of imaging devices use entangled light, accelerometers, magnetometers, electrometers, gravity sensors. These allow measurements of frequency, acceleration, rotation rates, electric and magnetic fields, photons, or temperature with levels of extreme sensitivity and accuracy.

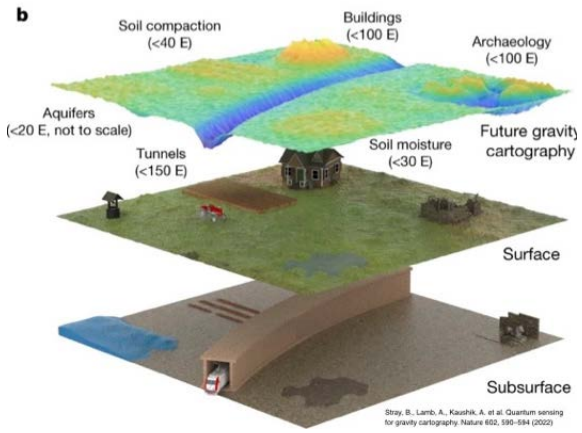
These new sensors use a variety of quantum effects: electronic, magnetic, or vibrational states or spin qubits, neutral atoms, or trapped ions. Or they use quantum coherence to measure a physical quantity. Or use quantum entanglement to improve the sensitivity or precision of a measurement, beyond what is possible classically.



Quantum Imaging applications can have immediate uses in archeology, and profound military applications. For example, submarine detection using quantum magnetometers or satellite gravimeters could make the ocean transparent. It would compromise the survivability of sea-based nuclear deterrent by detecting and tracking subs deep underwater.

Quantum sensors and quantum radar from companies like Rydberg can be game changers.

Gravimeters or quantum magnetometers could also detect concealed tunnels, bunkers, and nuclear materials. Magnetic resonance imaging could remotely ID chemical and biological agents. Quantum radar or LIDAR would enable extreme detection of electromagnetic emissions, enhancing ELINT and electronic warfare capabilities. It can use fewer emissions to

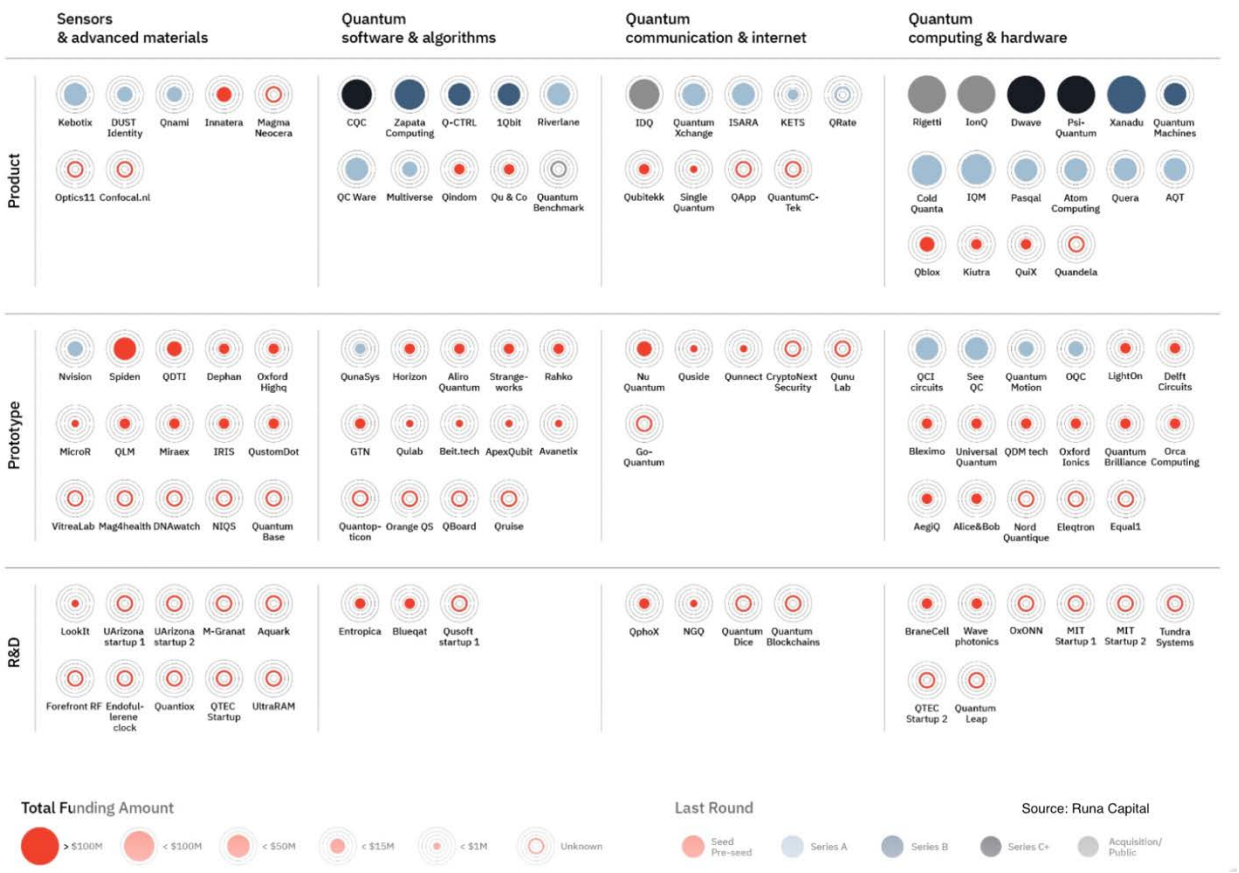


get the same detection result, for better detection accuracy at the same power levels - even detecting stealth aircraft.

Finally, *Ghost imaging* uses the quantum properties of light to detect distant objects using very weak illumination beams that are difficult for the imaged target to detect. It can increase the accuracy and lessen the amount of radiation exposed to a patient during x-rays. It can see through smoke and clouds. *Quantum illumination* is similar to ghost imaging but could provide an even greater sensitivity.

National and Commercial Efforts

Countries across the world are making major investments ~$24 billion in 2021 - in quantum research and applications.



Lessons Learned

- Quantum technologies are emerging and disruptive to companies and defense
- Quantum technologies cover Quantum *Computing*, Quantum *Communications* and Quantum *Sensing and Metrology*
    - Quantum *computing* could obsolete existing cryptography systems.
    - Quantum *communication* could allow secure crypto key distribution and networking of quantum sensors and computers.
    - Quantum *sensors* could make the ocean transparent for Anti-submarine warfare, create unjammable A2/AD, detect stealth aircraft, find hidden tunnels and weapons of mass destruction, etc.
- A few of these technologies are available now, some in the next 5 years and a few are a decade out
- Tens of billions of public and private capital dollars are being invested in them
- Defense applications will come first
- The largest commercial applications won't be the ones currently think they're going to be
    - when they do show up they'll destroy existing businesses and create new ones