QUANTUM CYBERSECURITY

Del Rajan, PhD Candidate, VUW

SUMMARY

- A large scale quantum computer would break the digital security infrastructure
- Global investments in the billions
- Post-quantum and quantum cryptosystems are being developed

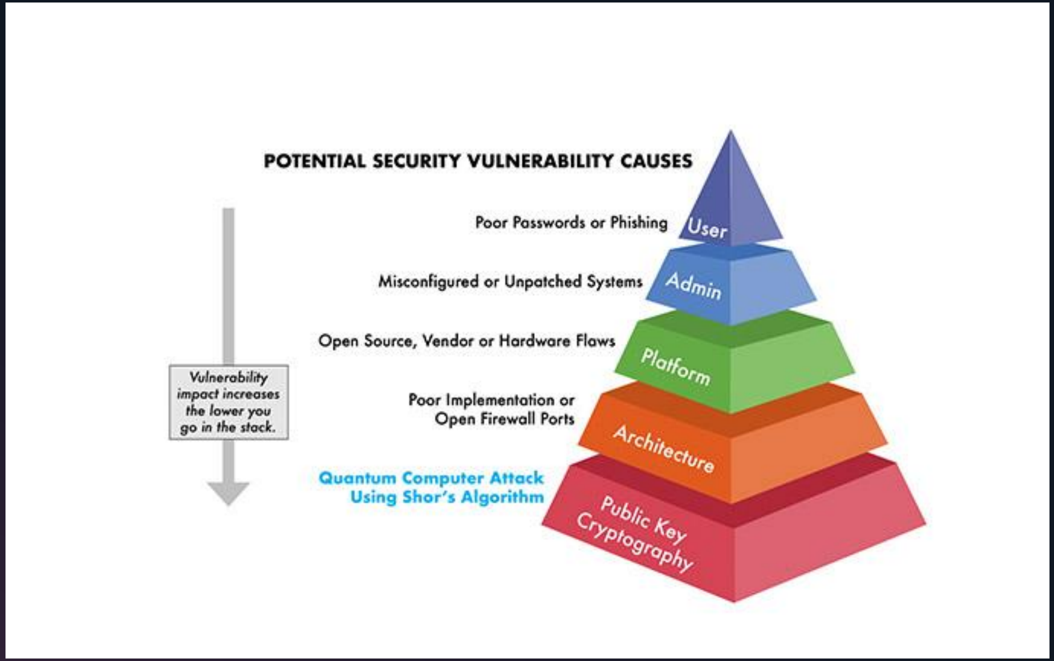
Source: IBM

Forbes article

- Title: “Schrodinger's Encryption: What The CISO Needs To Know About Quantum Cybersecurity”
- “Cybersecurity is constantly evolving, and the role of the Chief Information Security Officer (CISO) has to evolve in parallel”
- “...the CISO needs to get a handle on the quantum threats and opportunities...”
- “ ...Del Rajan and Matt Visser, propose a conceptual design for a quantum blockchain to resolve this threat”

Source: Forbes

QUANTUM COMPUTER


POTENTIAL SECURITY VULNERABILITY CAUSES
Poor Passwords or Phishing
User
Misconfigured or Unpatched Systems
Admin
Open Source, Vendor or Hardware Flaws
Platform
Vulnerability impact increases the lower you go in the stack.
Poor Implementation or Open Firewall Ports
Architecture
Quantum Computer Attack Using Shor's Algorithm
Public Key Cryptography

Source: ISARA (December 2018)

Shor's algorithm breaks public key cryptography

- Public key cryptography is based on integer factorization
- Thought to be impossible to solve in a reasonable time
- In 1994, MIT Mathematician Peter Shor showed that a quantum computer would be able to solve it very quickly

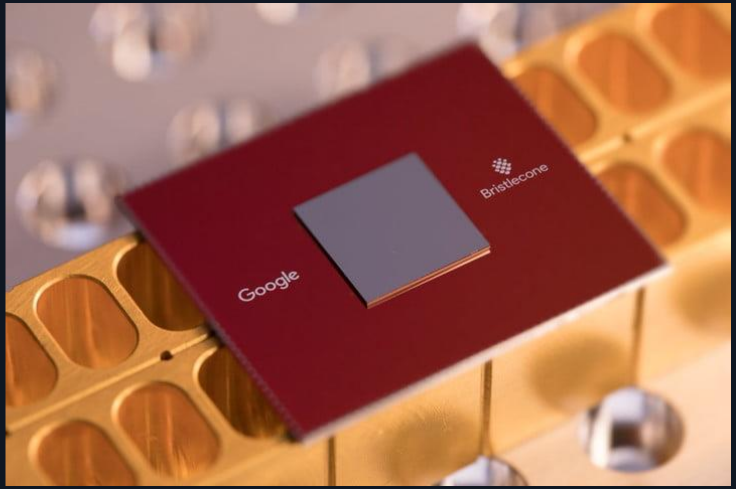
COMMERICAL PROGRESS

Commercial companies developing quantum computers include IBM, Google, Microsoft, Alibaba, and many more

IBM Q

Source: IBM Research

Google's Bristlecone



Source: Google AI blog

DIFFERENT TYPES

Quantum computers come in various forms

Gate model

Can break encryption
(IBM, Google)

Quantum Annealer

Solves one specific problem
(D-Wave systems)

Topological

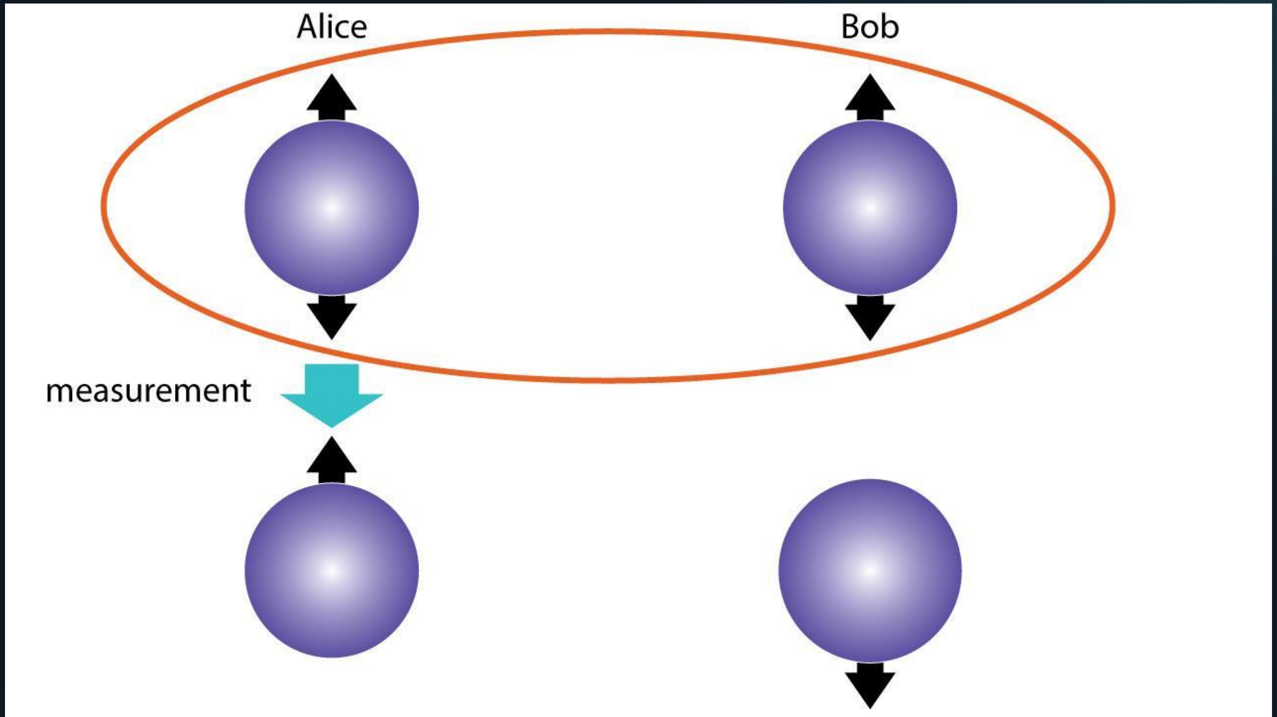
Less popular approach
(Microsoft)

One-way

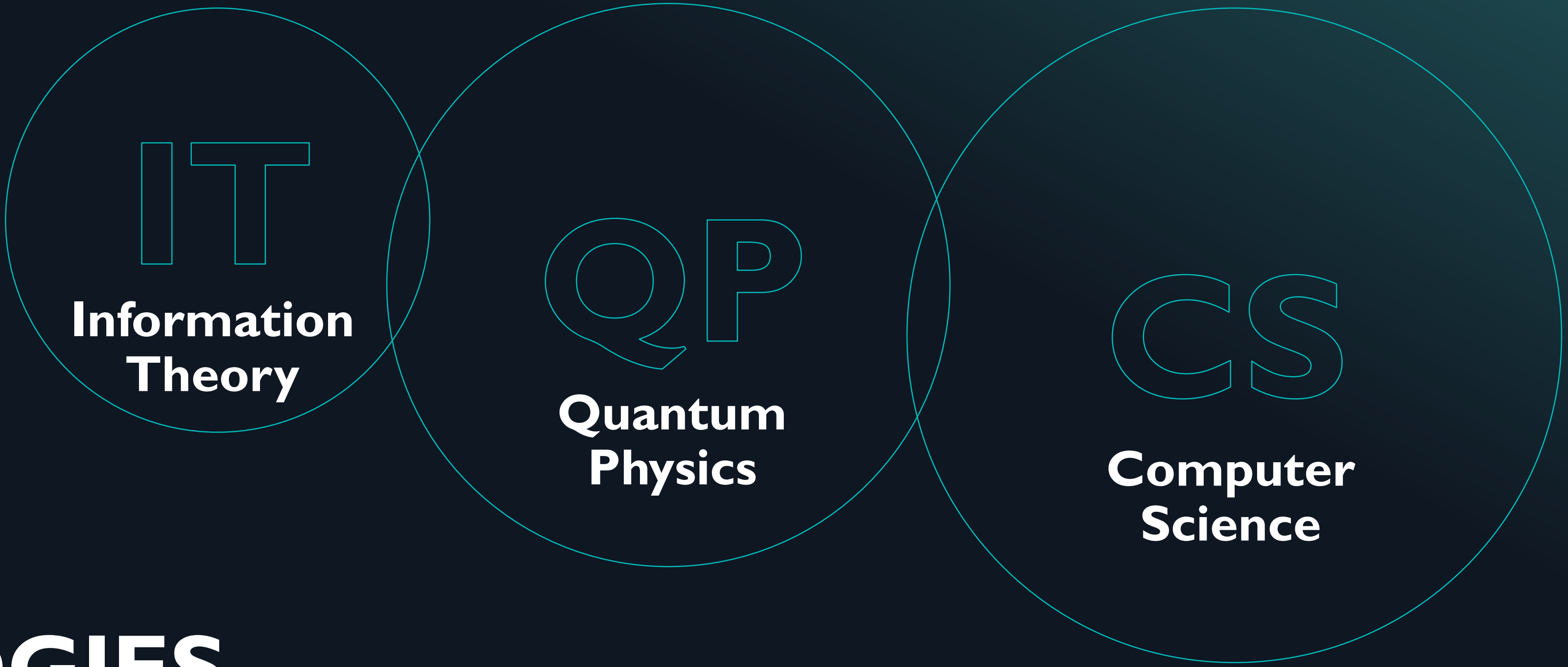
Less popular approach

QUANTUM PHYSICS 101

- Roughly speaking, the modern physics of particles (electrons, photons, etc)
- Most accurate theory known in all of science (experimental agreement to within ten parts in a billion)
- Exhibits shocking phenomena such as entanglement-in-space
- Quantum computer uses entanglement for its computational power
- More broadly speaking, quantum information technologies directly use quantum phenomena as part of its IT capabilities



Source: Science Magazine



IT

Information Theory

QP

Quantum Physics

CS

Computer Science

QUANTUM TECHNOLOGIES

Also known as quantum information technologies or quantum information

Quantum technologies

I

Quantum computers

Solves very hard problems

II

Quantum communications

Includes quantum cryptography

III

Quantum metrology

Ultra precise sensors

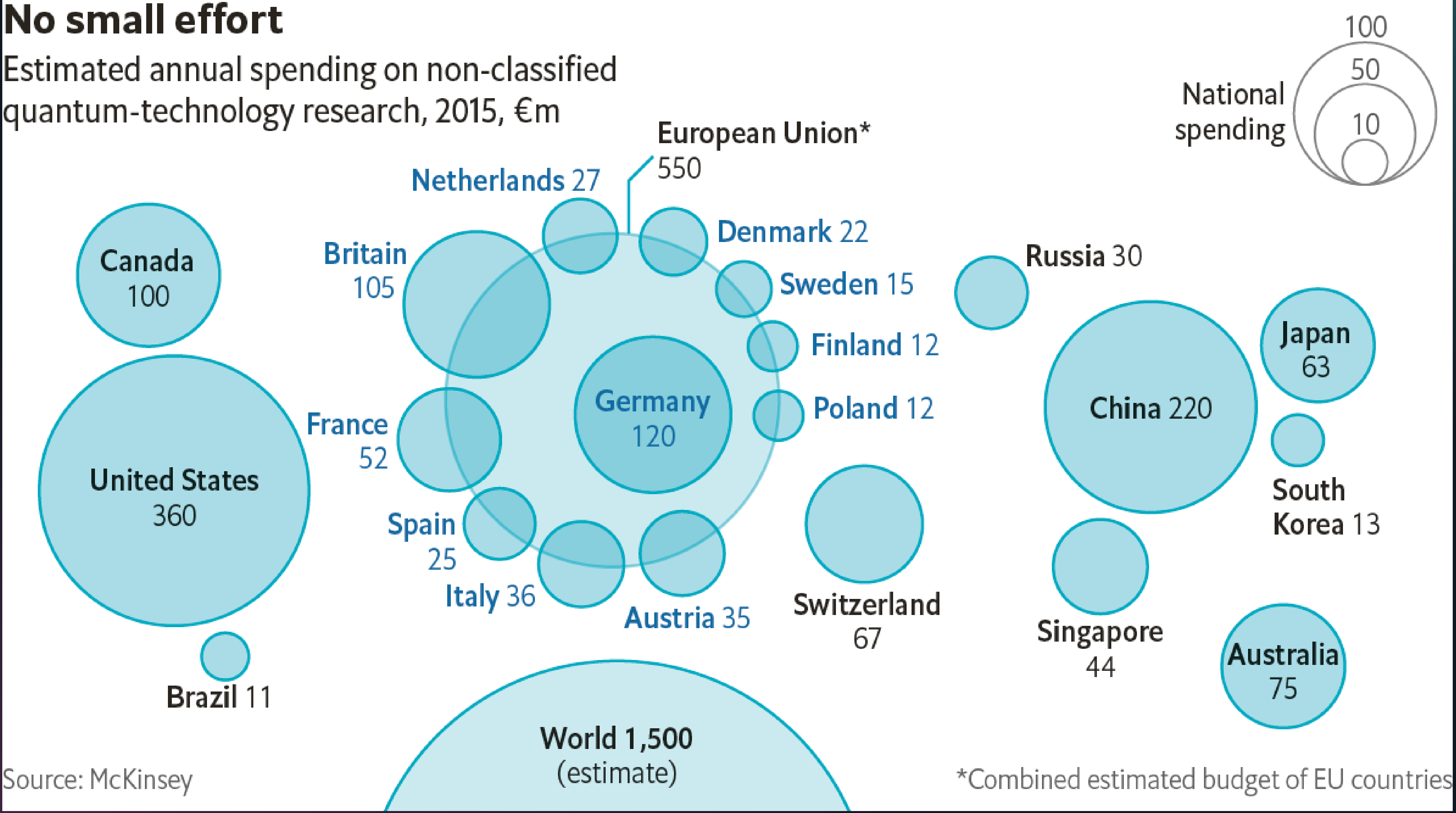
IV

Quantum blockchains

Secures blockchains

No small effort

Estimated annual spending on non-classified quantum-technology research, 2015, €m



Source: McKinsey

*Combined estimated budget of EU countries

UPDATED FIGURES

For China, US, and EU

1

China $10 billion

- $10 billion National Laboratory for Quantum Information Sciences
- Already a leader in quantum communications (Micius)
- Pan Jianwei, China's lead quantum information scientist, was on 2018 TIME's 100 Most Influencial People

2

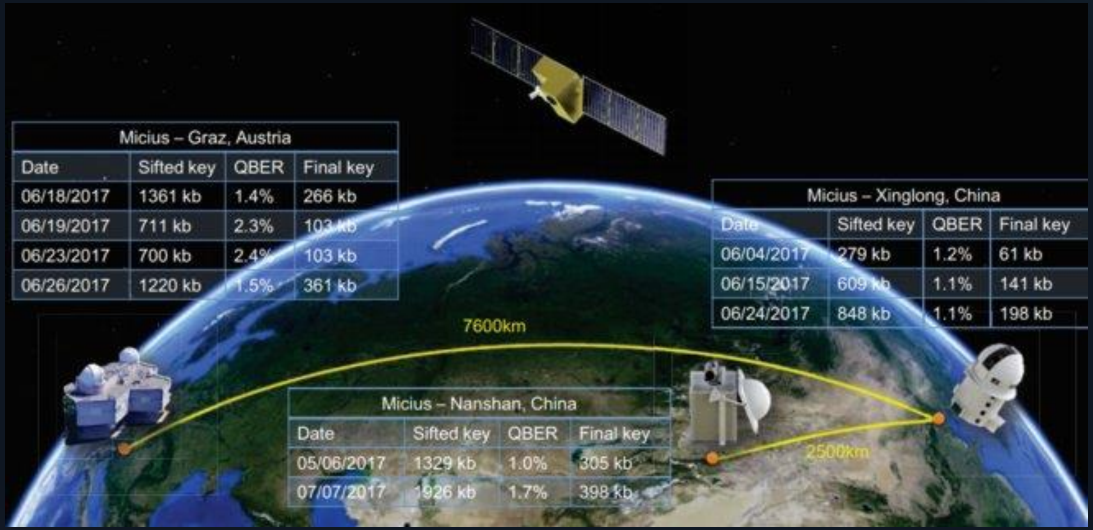
US $1.2 billion

- National Quantum Initiative Act
- Signed into law Dec 2018
- "…establish a federal program to accelerate U.S. QIS R&D…"
- "…concerns that China may be closing the gap with the United States in advanced technology R&D…"

3

EU €1 billion

- European Flagship on Quantum Technologies
- On top of the EU funding, an additional €650 million from Germany
- UK has its own £270 million National Quantum Technologies Programme



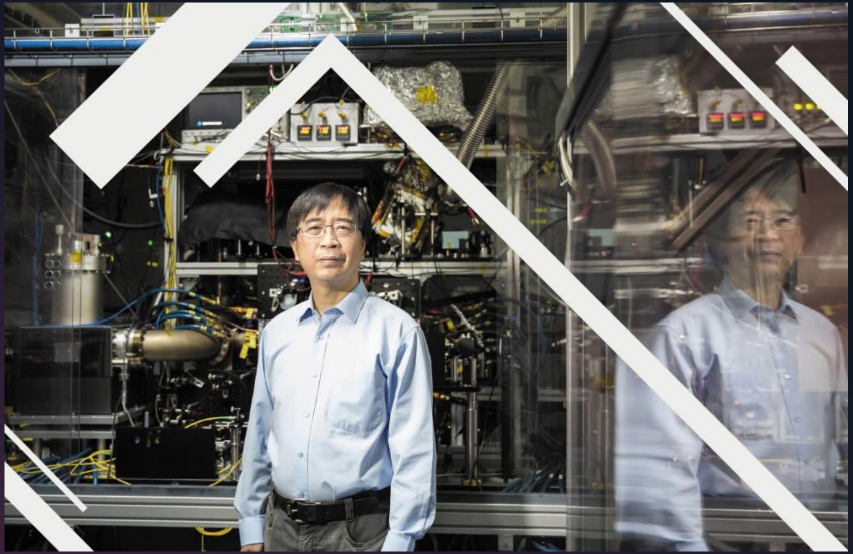
Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

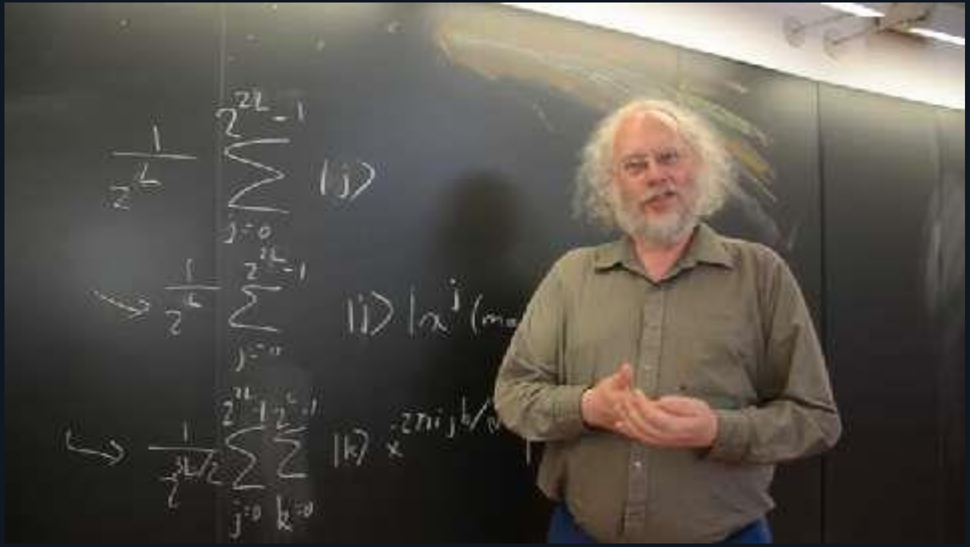
Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

Source: Physical Review Letters

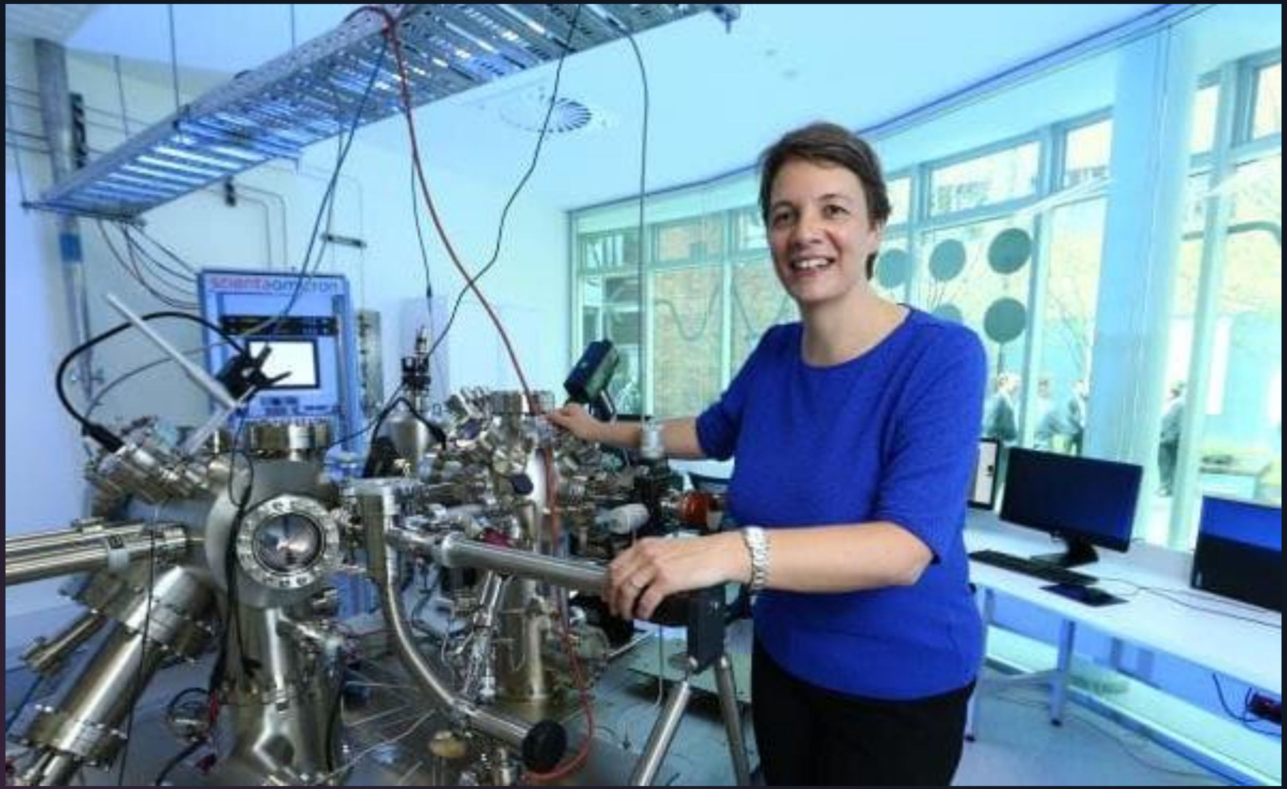
Source: White House / OSTP Photo via Twitter



Source: Chinese Academy of Sciences



Source: Physics World



Source: The Australian

AUSTRALIA

More closer to home

- Federal government investment for quantum technologies is around AUD$130 million
- Defense has established a ‘Next Generation Technology’ fund with quantum technologies as one of its seven priority areas
- Private quantum technology companies such as Quintessence (investors include Westpac Group)
- 2018 Australian of the Year was awarded to Prof. Michelle Simmons, a director of a quantum computing institute

SOLUTIONS

Defense against quantum computer attacks

Post-quantum cryptography

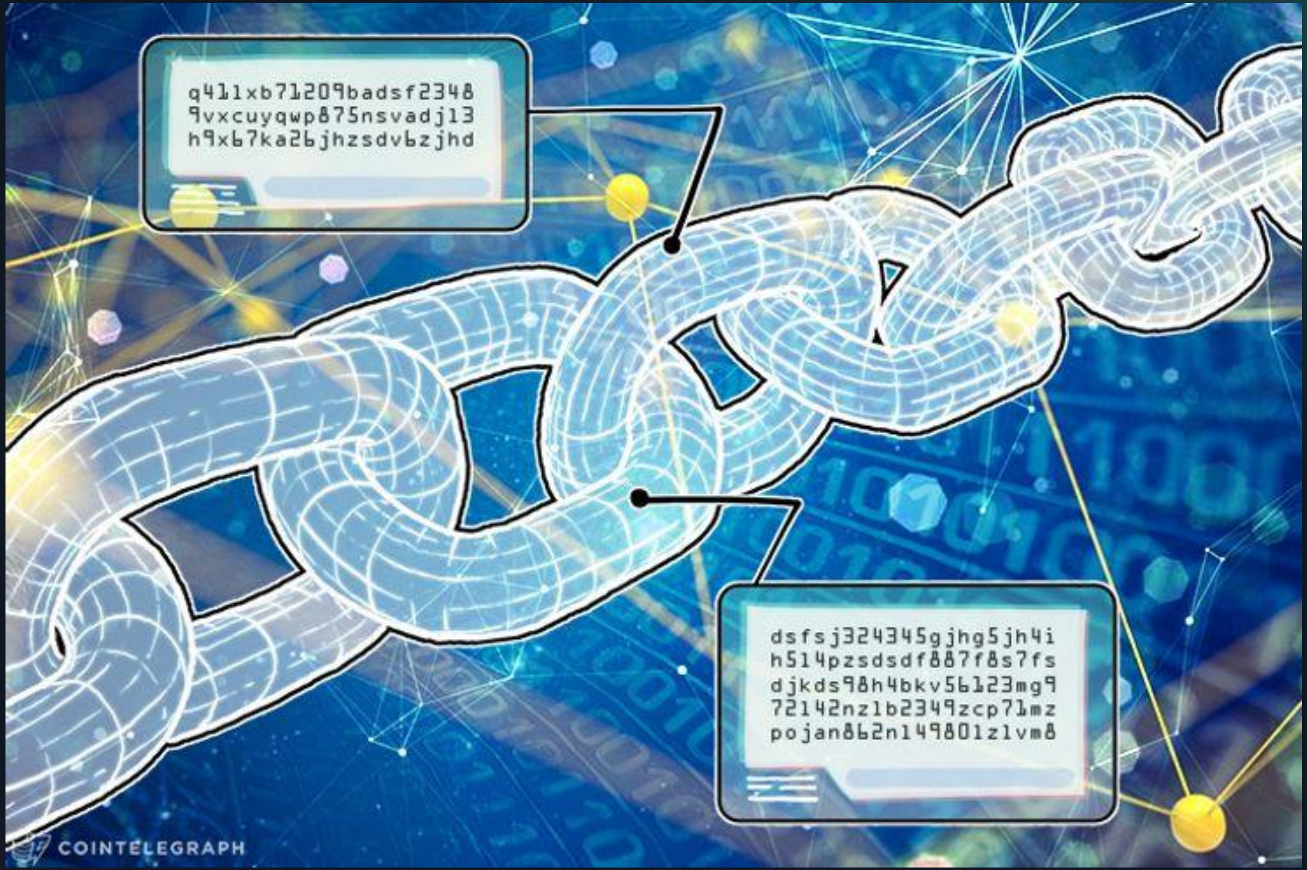
- Software solutions (uses hard math problems that are thought to be unsolvable by a quantum computer)
- Not a large change in infrastructure, but durability can be questioned as quantum computing capabilities increase
- NSA and NIST standardization process kicked off in 2015. Drafts standards expected 2023-2025.

Quantum cryptography

- Hardware based solutions (uses quantum particles to do the encryption; a form of quantum information technology)
- Secure by the laws of physics but a large change in infrastructure
- Quantum cryptographic solutions are on market today (Quintessence, ID Quantique, etc).
- Forms the valuable part of a quantum communications network
- Scalable networks are being developed in the US, China, Europe, etc

BLOCKCHAIN 101

- Blockchain system is composed of the blockchain data structure and a network consensus algorithm
- Blockchain data structure is the database
- Blocks linked in a 'chain' through cryptographic hash functions
- Consensus algorithm provides decentralization component (e.g. PoW)
- Used by IBM, Wal-Mart (food safety), Maersk (global shipping), etc



Source: Cointelegraph

BLOCKCHAIN

Quantum computers pose a security threat

1

Post-quantum blockchain

- Post-quantum cryptography
- Easier to implement
- Durability can be questioned

2

Quantum-secured blockchain

- Traditional blockchain system
- Adds quantum cryptography as a subcomponent
- Experimentally realized

3

Quantum blockchain

- In my PhD, redesigned a blockchain into a quantum information technology
- Protection using temporal properties of quantum particles (entanglement-in-time for 'chain'), and quantum network for the decentralization piece
- Featured on Forbes, IEEE Spectrum, MIT Tech Review
- This research is in the top 5% of all research outputs ever tracked by Altmetric (99th percentile)

THANK YOU!

Del Rajan

Email:
rajandel@myvuw.ac.nz

Website:
http://sms.victoria.ac.nz/Main/GradDelRajan