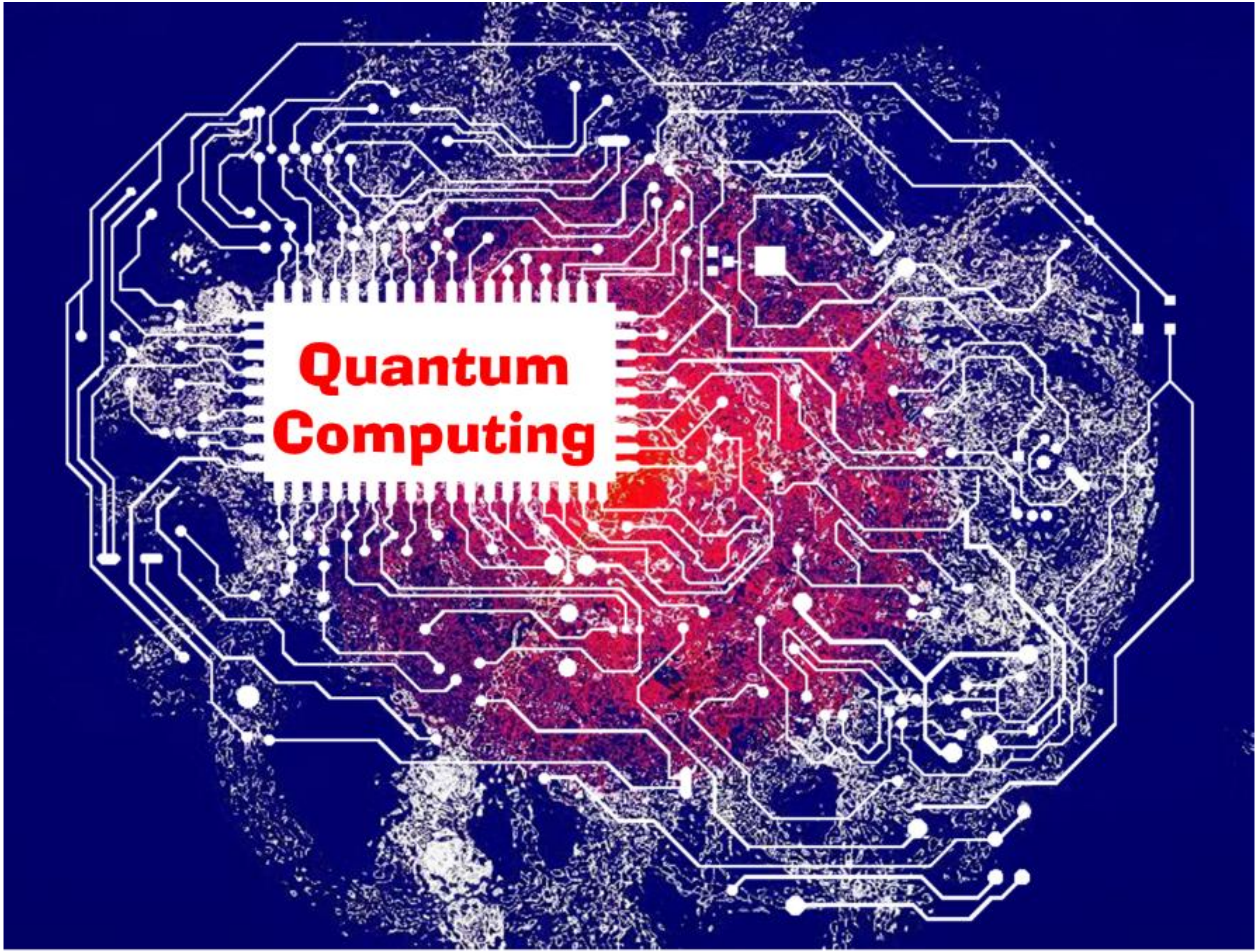


VC investment analysis

Quantum Computing

April 2018

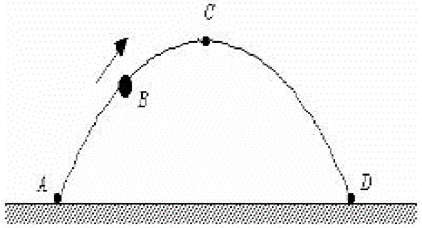
Julian Diederichs
Ritika Goyal
Gonzalo Laffitte
Michael Mueller
Rafael Scaglia de Paula

Table of contents

1. Quantum computing as an alternative to classical computing was thought up by Feynmann in 1982

In the macroscopic world the laws of classical mechanics rule

Isaac Newton
(1643-1727)



$$F_m = ma; \quad a = \frac{d^2x}{dt^2}$$

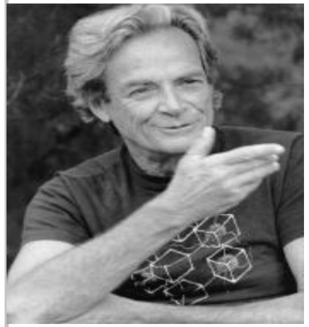
Characteristics of classical behavior:

- **Deterministic:** end result of a physical situation can be predicted deterministically and is always the same given equal starting points.
- **Causal:** action is reaction – one thing leads to another.

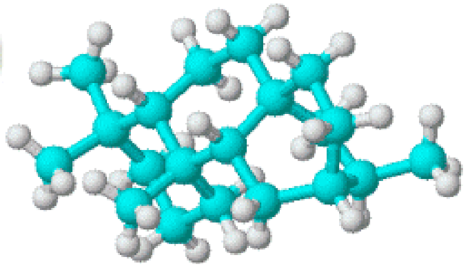
Classical computing is ruled by classical mechanics, but it has limits:

- **Moore's/Amdahl's Laws:** Number of transistors doubles every 24 months. Benefits of parallelization.
- **Limit:** As transistors' size reaches the size of an electron, it's behavior is governed by quantum mechanics, not classical.
- **When:** Current commercial size is 5nm transistor. 1-3 nm is predicted as limit and that will happen as soon as 2022.

On a subatomic scale, the laws of quantum mechanics rule



Richard Feynmann
(1918 –1988)



$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

Characteristics of quantum mechanics:

- **Superposition:** object can have multiple states simultaneously
- **Entanglement:** quantum states of particles are correlated even though spatially separated
- **Measurement paradox:** measurement affects outcome, there is no single outcome unless it is measured

How quantum mechanics can be the answer to the limits of classical:

- **Storage:** 20 q-bits can store a million variables in parallel.
- **Reading time:** as q-bits values are correlated, reading just one gives you information about the rest.
- **Calculations:** Using superposition and entanglement, quantum computers can calculate all possible calculations solutions at once.

2. Only since 2014 we have seen a massive uptake of industry interest and funding in the field of quantum computing

Hardware | **Software**

2015: Software R&D and innovation

1999 Hardware R&D and innovation starts

2014-2017 Hardware R&D budgets rise to $ billions

1999
EU invests €50-75 M in quantum technologies via FET program over next 7 years

2004
USA ARDA invests in Quantum Information Science and Technology Roadmap

2010
Canadian government invests €78 M in quantum technologies over next 7 years

2013
Lockheed Martin buys D-Wave Two[1]

July 2014
IBM invests $3 B in research initiative that includes quantum computing

2015
Chinese government plans significant investment in quantum computing

2017
Quantum computer hardware startup raises Series A at $18M

2018
Google introduced first 72 qubit chip – highest number yet used

2000 | 2005 | 2010 | 2015 | 2017 | 2018

2001
SK Telecom starts R&D on quantum communication

2005
Microsoft starts Station Q at UC Santa Barbara

2011
Lockheed Martin buys D-Wave computer for $10M

Dec 2013
UK Government invests €370 M in quantum technologies in next 5 years

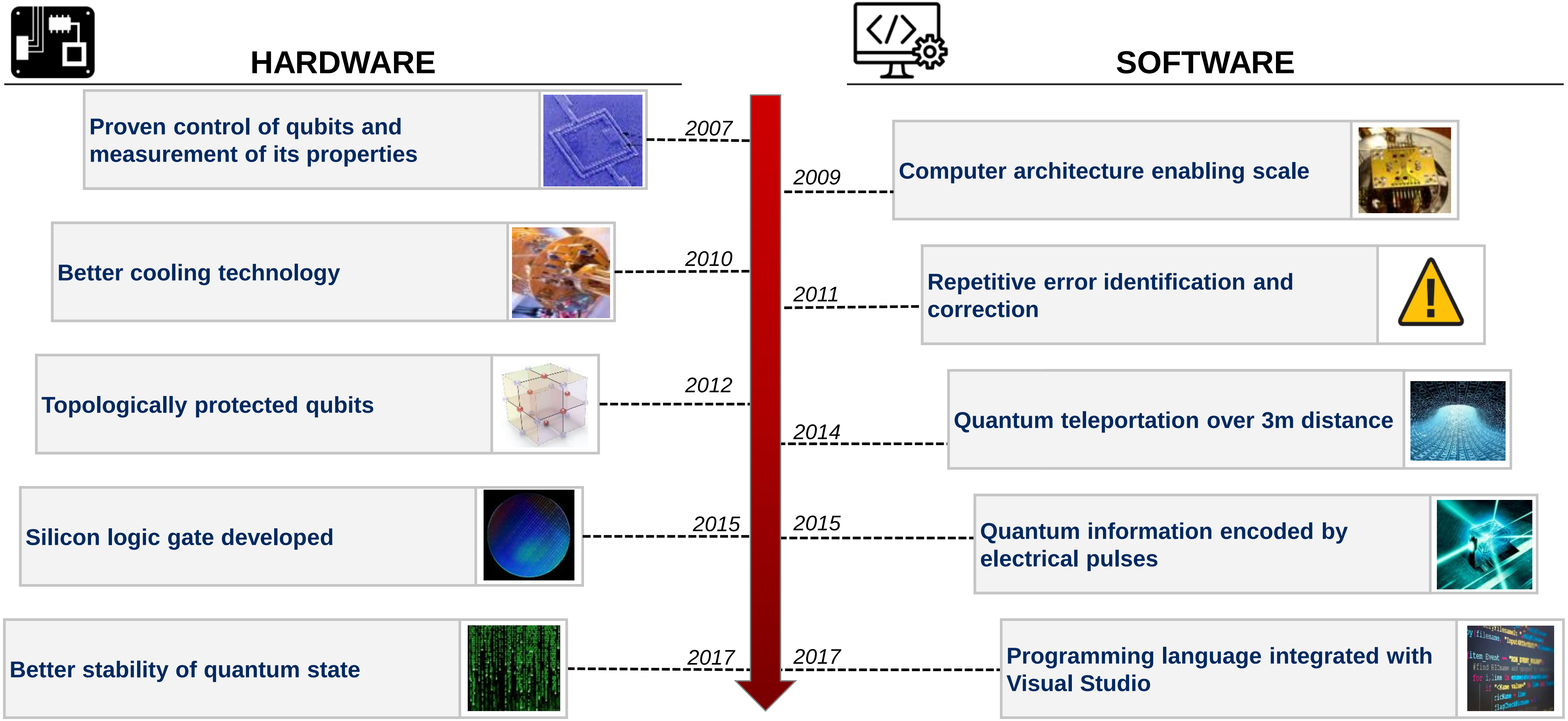
Sep 2014
Google ab-sorbs John Martinis' research group (UC Santa Barbara)

Sep 2015
Intel invests $50 M in QuTech Delft to develop a quantum computer

2016
IBM makes Quantum platform accessible for researchers and developers

2018
D-Wave secures $50M to bring quantum computing to the cloud

3. Recent investments in scientific and technological developments have brought feasibility and application of quantum technology closer

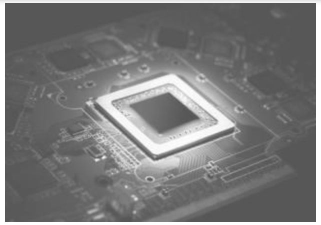


Notes: Non-exhaustive selection of developments (other developments can be found online https://en.wikipedia.org/wiki/Timeline_of_quantum_computing)
Source: Internal research

4. However, experts believe that universal quantum computing is not going to be viable in the next five years

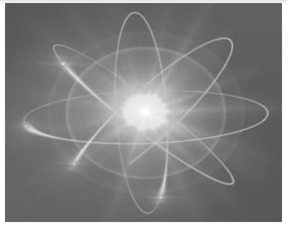
What is needed to have a commercially available quantum computer?

Processing power (Qubits quantity)



- **Large number of** qubits for **processing power** and **error correction**

Stability (Quantum coherence)



- Protection of **quantum state from decoherence** during calculation and measurement in **large scale systems**

Quality (Error correction)

- **Error identification** and **correction** to assure a confident output from calculations in **large scale systems**

Experts' opinions:

"To be useful (logic + error correction) a quantum computer would need at least 1 million qubits! I cannot see it happening in the next 10 years"
Visiting Professor and Principal Investigator,
Centre of Quantum Technologies at NUS

"Decoherence is the biggest obstacle today. Today we can maintain a quantum state for just a few microseconds"
Visiting Professor and Principal Investigator,
Centre of Quantum Technologies at NUS

"We have seen experiments demonstrating quantum error correction on small systems. A universal error-tolerant quantum computer is still a long way off"
Visiting Professor and Principal Investigator,
Centre of Quantum Technologies at NUS

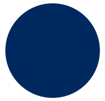
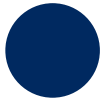
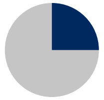
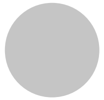
"It is hard to say when we are going to see an useful quantum computer. It may happen in 5 years, it may happen in 15."
Associate Professor and Principal Investigator,
Centre of Quantum Technologies at NUS

"In the beginning it was a physics problem, but today is an engineering problem. The greater the number of qubits, the harder it gets to isolate the system"
Visiting Professor and Principal Investigator,
Centre of Quantum Technologies at NUS

"QC 'real advantage' will happen with +1000 error corrected qubits. My expectation is 5 to 15 years."
CEO,
Quantum software Startup

Source: Experts' interviews

5. Processing power and quantum physics drive use cases of quantum computing – algorithms for which have been around for +20 years

#	Use cases		Description	Development Reason & Current stage	Current Challenges & Barriers	Maturity of algorithms	and key players
1	**Quantum Simulation**		• Special purpose quantum systems used for **simulating behavior of quantum mechanical systems**, i.e. molecules, materials	• Molecules' simulation is a **quantum mechanics** problem and suitable for **quantum computer** • **Mathematical** formulation of algorithms is **well-known** among scientists and professionals • **Largest** molecule simulated (BeH_2) has **only 3 atoms and used 6 qubits**	• Larger molecules would need a **massive number of qubits**: caffeine, with 24 atoms, would require ~1000 qubits • Results are not perfect due to **errors in quantum calculations**		• Universities' research departments • Corporations (eg. Google, Microsoft, IBM)
2	**Encryption (Prime factorization)**		• Prime factorization in order to **break encryption** and get access to (military) intelligence	• **Mathematical** formulation of algorithms that crack encryption are **well-known** • Current algorithms, such as Shor's Algorithm (formulated in 1994), can break **RSA cryptography** (widely used for secure data transmission)	• Need for **qubit scalability:** a RSA-15 key requires 5 qubits to have a confidence level of 99% • Terabyte-size RSA keys may require **large amounts of time** in a quantum computer		• Universities' research departments • Corporations (eg. Google, Microsoft, IBM) • Governments' intelligence and security departments
3	**Big Data computing**		• Applications for **data mining (Big Data)**, **machine learning** and **optimization problems** applied to the most suitable for quantum computing problems	• **Algorithms** have been **proposed**, but just a few have been through an **implementation tentative** (still few proof-of-principle demonstrations) • Currently **few wide-spread algorithms**, such as Grover's searching database algorithm	• **Large number of qubits**, with improved characteristics • **Error still high**: need to achieve error correction threshold by increasing number of **error-correcting qubits**		• Universities' research departments • Corporations (eg. Google, Microsoft, IBM) • Governments' intelligence and security departments
4	**General purpose computing**		• **General purpose** computing that allow generic algorithms for different types of problems	• There is **no existence** of general purpose machine • **No algorithms** in different class of problems than previously stated	• **Large number of qubits**, with improved characteristics • **Error-correcting qubits** to improve precision and reduce noise • General purpose **suitable problems** for quantum computing algorithms		• N/A

Quantum physics Processing power

Source: Companies' and Universities' website, Internal research

6. Based on quantum characteristics, specific application fields are suitable for QC adoption

		STATUS QUO – CLASSICAL	QC VALUE-ADD	QC DEVELOPMENTS
Q Chemistry	Catalyst reactions and Material Discovery	Classical computing limit is at a molecule with 50 electrons, with errors.	Molecules are formed following quantum mechanics' laws. Quantum computers inherently show quantum characteristics and are expected to model larger molecules in the future.	Simulation to date limited to small molecules (beryllium hydride, lithium hydride, and hydrogen)
Q Chemistry	Drug development	Trial and error - it takes pharmaceutical companies up to 10+ years and billions of dollars to discover a new drug and bring it to market.	Understanding the interactions of drugs with proteins will be much more accurate, faster and cost effective by harnessing the power of QC	Biogen, Accenture and 1Qbit have show-cased in a joint effort the potential to speed up drug discovery for diseases such as multiple sclerosis, Alzheimer's and Parkinson's.
Optimization	Cyber Security	Significant share of encrypting currently based on RSA and Elliptic-curve cryptography.	Shor's algorithm can solve the factorization problem, but requires powerful computing, such as QC.	Technology resistant to Quantum hacking is being developed already by top universities and startups. The flipside is the increased security that could be offered and needed with quantum-based cryptography.
Optimization	Supply Chain and Logistics	Classical computing at its limit trying to solve large scale optimization problems.	Quantum gates are able to produce all possible solutions at once using entanglement and superposition.	Research to date limited to study and development of algorithms for semi-definite problems, but not implementations or test cases to date.
Optimization	Financial Modelling	Advanced portfolio optimization (returns, risk) done using time-intensive and inefficient Montecarlo simulations	Quantum gates are able to produce all possible solutions at once using entanglement and superposition.	Current size of problems that can be solved is small. Optimizing a portfolio of 3 assets already requires 84+ qubits – 1Qbit experiment
Optimization	Artificial Intelligence and Machine Learning	Classical computing at its limit trying to solve large scale AI/ML problems	QC enabled algorithms, such as Grover, can accelerate data based search problems.	Enormous potential for applications such as Voice, Image and writing recognition. Use cases: Lockheed Martin (autopilot), Google (Self-driving)

Source: Internal research, Companies' websites

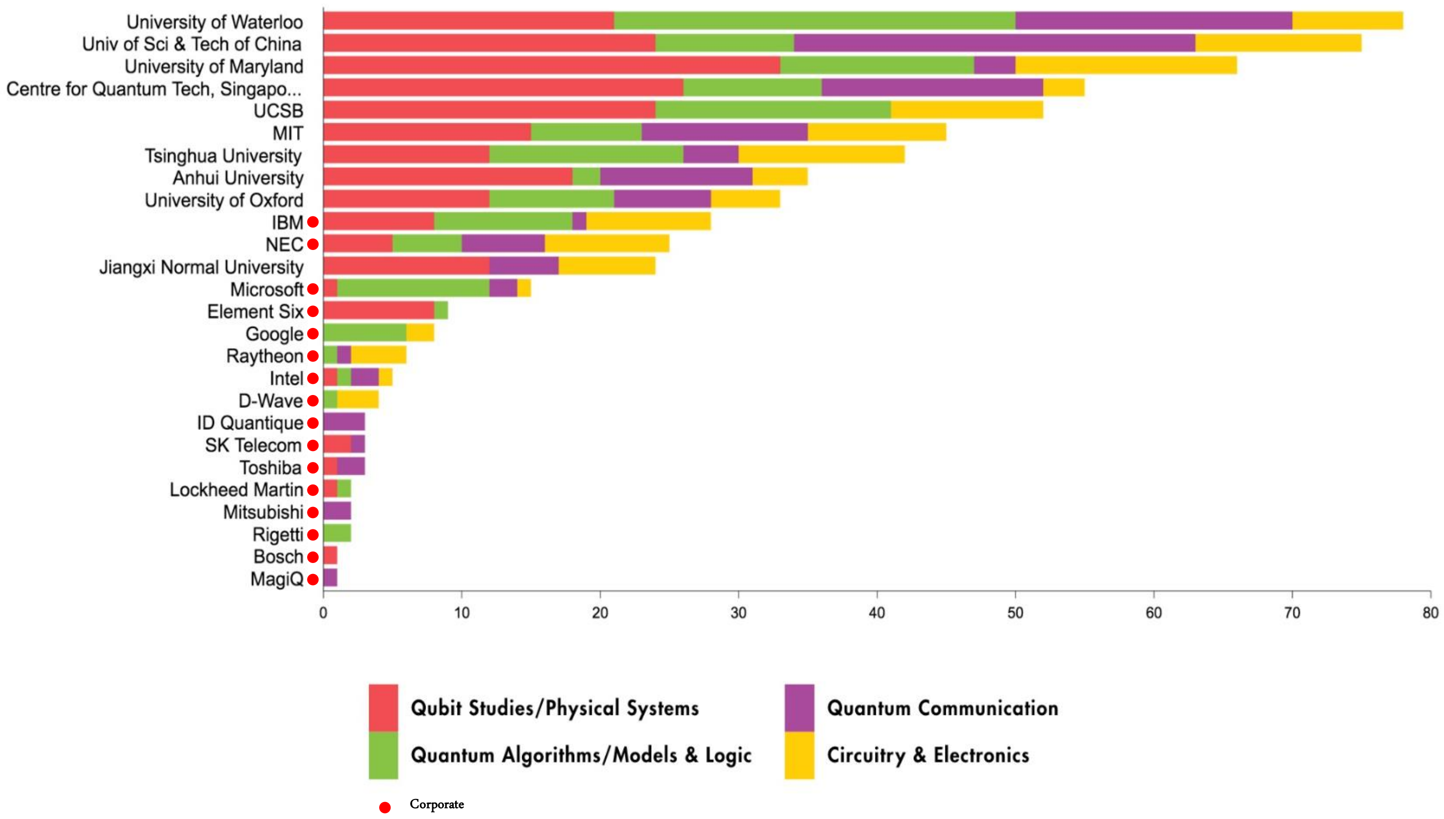
7. Technology incumbents are getting involved in QC activities, increasingly also on the software side

	Companies[1)]	Recent headlines	Role in the quantum computing ecosystem	HW	SW
US tech incumbents	Google	▪ Released **Bristlecone** a 72 qubits system, in 2018 ▪ Started **Google's Artificial Intelligence Lab** in partnership with John Martinis' research group and NASA in 2014	▪ Currently one of the strongest player in the ecosystem with its proprietary research and its investment in D-Wave	✓	✓
	Microsoft	▪ Recently previewed a **quantum computing development kit** ▪ Started own research center **Station Q** in 2005 at UCSB and supports several research groups around the world to develop a reliable topological qubit	▪ Microsoft has been working on full-stack solutions including hardware platforms, software and programming languages/ SDKs	✓	✓
	IBM	▪ Announced a **50 qubits** system in 2017 ▪ Has **in-house quantum research group** which aims to develop an end-to-end quantum computer based on superconducting qubits	▪ Seeks to be a leader in QC ecosystem and wants to drive developers to their cloud platform with SDK	✓	✓
	intel	▪ Announced a **49 qubit system** in 2018 ▪ Starts a ten year intensive **collaboration with QuTech Delft** in 2015 to develop a fault tolerant quantum computer	▪ Seeks to be the leader for quantum computing chips, however covers full stack through collaboration with QuTech	✓	✓
	Hewlett Packard Enterprise	▪ Runs a **Quantum Information Processing (QIP) Group** in their HP lab ▪ Focus on quantum computation, cryptography and teleportation/ communication	▪ *Limited information of HPE's strategy available*	✓	
China	Alibaba Group 阿里巴巴集团	▪ Cloud service subsidiary **Aliyun** ("Alibaba Cloud") and the Chinese Academy of Sciences jointly launched an 11-qubit quantum computing service, which is available to the public on the **Quantum Computing Cloud Platform**	▪ Compete for leading role in China, trying to establish standard with its cloud solution	✓	✓
	Baidu 百度	▪ Announced the launch of a **quantum computing institute** with over $15 billion funding for the next 5 yers ▪ Plan gradual integration of quantum computing in their core business	▪ Compete for leading role in China, currently far behind Alibaba		✓
Others	HITACHI	▪ Started the **Hitachi Cambridge Laboratory** in 1989 ▪ Publicly reporting activities in quantum experimental and theoretical research	▪ Currently focusing on basic research through Hitachi Cambridge Lab	✓	
	TOSHIBA Leading Innovation	▪ Develops technologies to make **Quantum Key Distribution** commercially available, including use of QKD over single optical fibre	▪ Aims to be a leader in quantum cryptography	✓	
	NOKIA Bell Labs	▪ Bell Labs is a leader in research on topological **quantum computational qubits** that would allow more robust quantum computers	▪ Focus on basic research	✓	

Notes: 1) Non-exhaustive selection of companies (other companies on the watch list include Lockheed Martin, Raytheon, Airbus, Amgen & Biogen)
Source: Company websites, desk research

8. Academic research in QC is led by North America and China – Singapore is recognized as global leader

Leading academic institutions & organizations in quantum computing
[# of publications; as of July 2017]



Additional information & comments

University of Waterloo, Canada: Institute of Quantum Computing (IQC) was launched in 2002 and initially funded by Mike Lazaridis (Founder of RiM/BlackBerry)1)

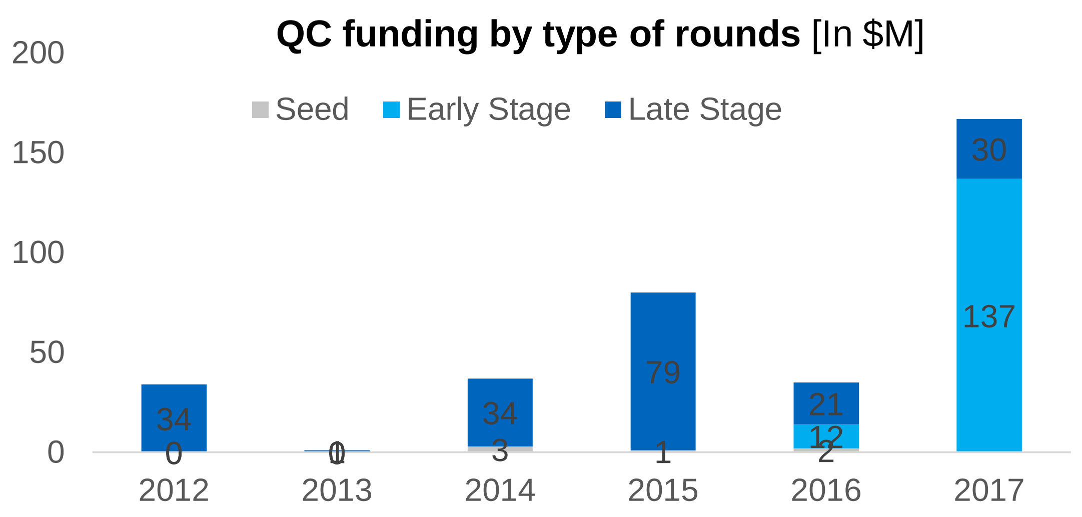
University of Science & Technology, Anhui, China: Leading institution in China under the leadership of Pan Jianwei ("Father of Quantum"), new quantum research supercentre with US$ 10 Billion funding to be opened in 2020

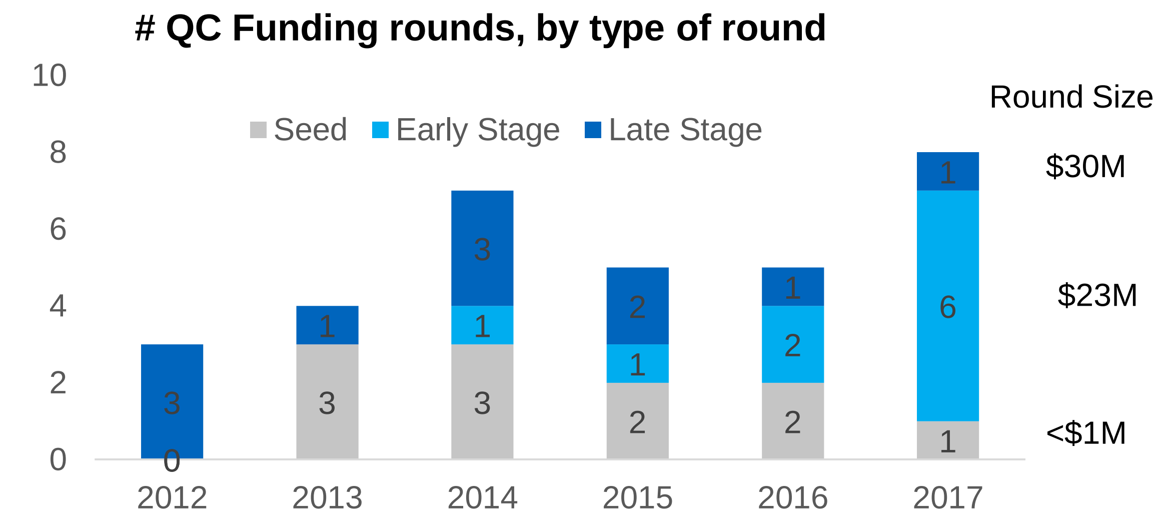
University of Maryland, USA: Joint Quantum Institute (JQI) is a leading US American research institute in Quantum Computing; Founded in 2006; less focus on Quantum Communication than IQC and USTC

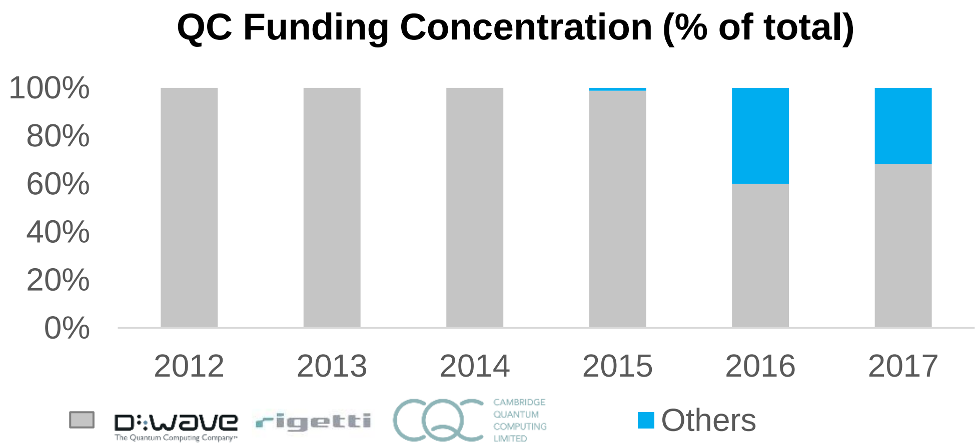
Corporate research centers of **IBM** (IBM Q)2) and **NEC** leading among non-academic institutions in number of publications

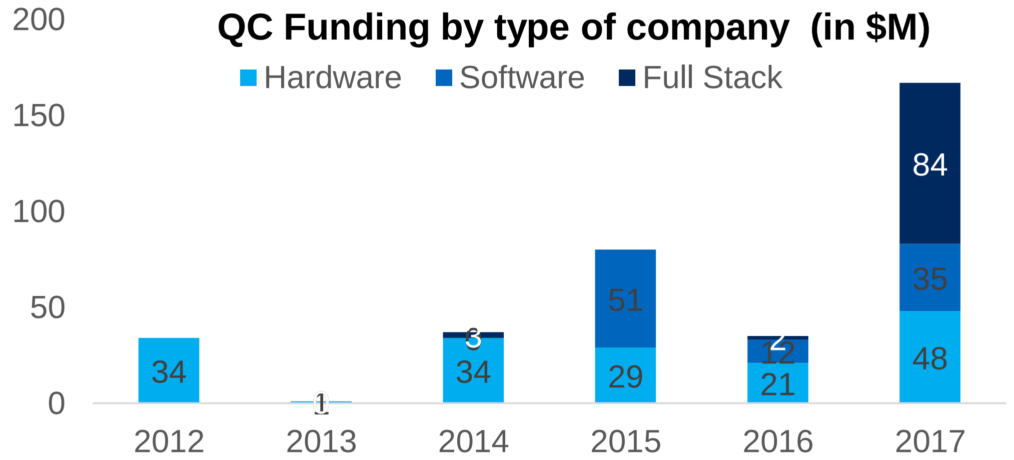
Notes: 1) As of January 1, 2017, IQC personnel includes 26 faculty members, three research assistant professors, 36 postdoctoral fellows and over 100 students 2) www.research.ibm.com/ibm-q/
Source: quid.com; Scopus; websites

9. Funding for QC startups is increasing over the years- with more software/full stack companies getting funded at seed and early-stage









Source: Secondary Research

10. Startup creation and funding in operating systems and data security apps space is on the rise

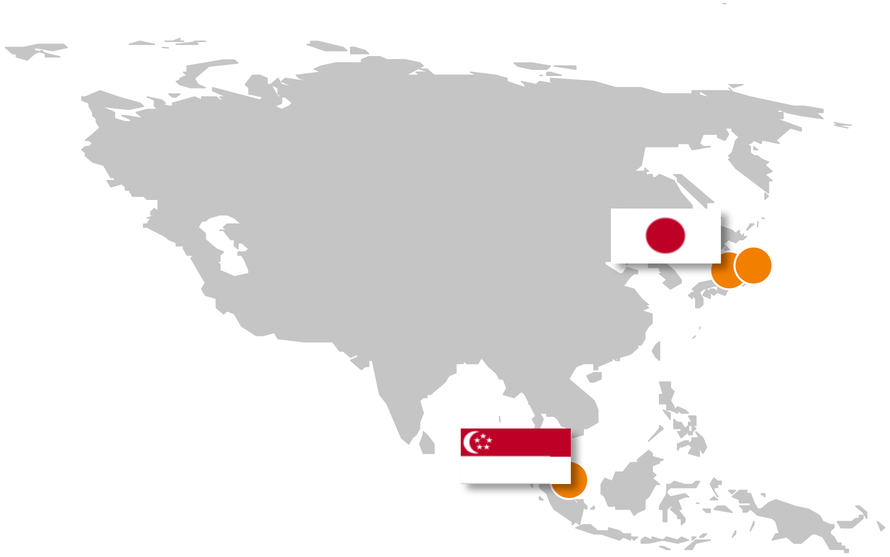
Category	Sub-Category	Type	US	China	ROW
Hardware	Quantum Computer	NA	• **Quantum Circuits (18)** (canaan partners, SEQUOIA)		• **D Wave Systems (17, 35, 134)** (Fidelity Investments, Goldman Sachs)
	Advanced Materials	NA	• Nano Meta Technologies (1.5) (Quantum Wave Fund)		
Software	Operating Systems	NA			• Cambridge Quantum Computing (50) (JSR)
	Applications	Data Security	• MagiQ (9) • Qxbranch (5) • Qubitekk (<1)		(Barclays Accelerator, Quantum Wave Fund) • Post Quantum (1.25, 10.3) • ID Quantique (10) • Quintessence Labs (2)
		Chemistry/Genomics			(INCJ, MUFG) • Quantum Biosystems (1, 4.4, 20.5)
	Computat'n Platforms	NA	• QC Ware (<1)		• 1QBit (35) (FUJITSU, accenture)
Full Stack	NA	NA	• **Rigetti (2.4, 24, 40)** • **IonQ (2, 20)** (NEA, Andreessen Horowitz, Founders Fund)		

Bold means funded by marquee investors e.g. Sequoia, A16Z, Goldman Sachs, Google Capital

Source: Secondary Research; Note: Numbers in brackets indicate amount raised till date in USD M: colors indicate seed, series A, series B. Included startups with ~$1M funding or above

11. Most QC start-ups in South East Asia and other Asian markets are in nascent stages

Desk research, VC databases and several interviews with quantum computing experts allowed us to identify only two early-stage start-ups, and one growth-stage startup in the target region



All startups in the region currently focus on software

	Tokyo Quantum Computing	HORIZON	QB
HQ	Tokyo	Singapore	Osaka
Year of founding	2017	2018	2013
CEO Profile	BS, MA & PhD (‘03), Physics, Tokyo Metropolitan University	PhD, University of Oxford (‘07), 5+ years at Centre for Quantum Technologies, Asst Prof at SUTD	MS, Analytical BioChem, University of Tokyo, MBA, Columbia University, McK, Innovation Network Corp of Japan
Investors ($ funded)	--	--	JAFCO, Mitsubishi UFJ Capital, Innovation Network Corporation of Japan ($26M)
Focus area	Computational software: Quantum annealer simulation software	Software dev tools to help engineers write applications for quantum computers	Low-cost, high-throughput, real time DNA sequencing platform based on quantum mechanics
Website	To-qc.com	Horizonquantum.com	Quantumbiosystems.com

Notes: 1) Quantum annealing (QA) is a metaheuristic for finding the global minimum of a given objective function over a given set of candidate solutions
2) Singapore University of Technology and Design
Source: Discussion with D-Wave scientist

12. All kinds of capital chasing QC startups- from traditional VC, government grants to venture debt- most not following a deep thesis at this point

NAME	COUNTRY	INVESTMENT THESIS	HW/SW	INVESTMENTS	INVESTMENT TIMELINE	AVG ROUND SIZE
ANDREESSEN HOROWITZ	USA	Full Stack approach- allows for rapid testing and pushing innovation on all fronts- chips, programming language, fab units	Full Stack	Rigetti (Series A, Series B)	2017, 2017	$24M -$40M
Data Collective	USA	Deep tech investments to transform existing giant industries	Full Stack	Rigetti (Series A, Series B)	2017, 2017	$24M -$40M
FOUNDERS FUND	USA	Focused on taking technology risk and funding revolutionary tech in – advanced machines/computing power/biotech	Full Stack	Rigetti (Series A, Series B)	2017, 2017	$24M -$40M
ALCHEMIST ACCELERATOR	USA	Accelerator with focus on B2B startups	Full Stack, Software	Rigetti (Seed) , QC Ware (Seed)	2014, 2015	<$1M
EPSRC Engineering and Physical Sciences Research Council	UK	Focused on hardware investments- in spaces where lab prototypes are already beating classical counterparts e.g. quantum sensors	Hardware	QT Hub for Sensors, Networked Quantum Information Technologies	2014, 2013	$100M-$400M grants
Quantum Wave Fund Riding the wave of quantum technology revolution	USA	Focused on investing in companies with developed products (not idea/research stage) in the QC space- specifically in areas of quantum encryption security, new materials and quantum devices.	Hardware , Software	Nano Meta Technologies (Seed), Quintessence Labs (Series A)	2013, 2013	$1-6M

Source: Secondary Research

13. Successful quantum computing software applications depend on superior algorithm performance, and close-to-market feasibility

For QC OS versatility is the key evaluation criteria

Software	Superior performance	Faster computing speed than classical comp.	Quantum Mechanics enabled modelling	Proprietary algorithms (no opensource)
	Feasibility	Theory/ formulas of algorithms proven	Clear target architecture	Robust Algorithms - runs on noisy QC systems
Operating system	Versatility	QC hardware agnostic	Existing developer/user community	Server interface functionality

14. Evaluation criteria matches success factors of current QC software startups

	Cambridge Quantum Computing	Post-Quantum
HQ	Cambridge	London
Year of founding	2014	2009
CEO Profile	BA Hons, Univ of London SOAS, Partner- Stanhill Capital Partners	BSc Civil Engg, MSc in Mgmt Science- Imperial College, Carlyle, JP Morgan
Investors ($ funded)	JSR Corporation ($50M)	AM Partners, Barclays Accelerator ($12M)
Focus area	Quantum computing O/S, compiler and some Applications in the field of Data Security	Quantum resistant data security solutions. Developed apps such as encrypted data sharing, enterprise-grade secure voice and messaging app, biometric authentication, quorum based consensus approval
Business Model	Licensing	Licensing + API as a service for some applications
Key Success Factors	• **QC Hardware Agnostic** - Modular design allows for optimization for each hardware type - Platform agnostic: works with all gate based platforms that generate, measure, manipulate qubits • **Robust Algorithms:** developed using a proprietary custom designed high speed supercomputer to accurately simulate a quantum processor	• **Prop algorithms**: 20 patents granted and pending approval for its technology • **Modular approach**: Targeting multiple industries/customers with host of modular solutions that can be mixed/matched • **Tech expertise**: crypto experts panel to pressure test algorithms for ‘cryptographic robustness’

Source: Secondary Research

15. Industry experts are aligned with academics that commercially viable QC is still a decade away

Academics | Industry

ADOPTION OF QC

- "QC advantage" will happen with stable (error corrected) qubits between 100-1000. Expectation: 10-15 years.
- OS development stands as a crucial enabler, not so much as a common platform but as a framework for developers (libraries, toolkits)
- **Since 1998 we hear that QC is going to play a big role in the near future.**
- **Since 2016 we feel in academia additional money and search for talents in the QC space – almost 50% of the Singaporean QC lab was hired by Chinese tech companies.**

AREAS OF APPLICATION

- The most likely areas of application in the near future are optimization (portfolio, schedule, logistics) due to low sensitivity to noise and error.
- **Grover's algorithm enables quadratically faster large scale database search and could disrupt recommendations systems, machine learning and risk management.**
- **New quantum safe encryption standard to be defined next year, driving adoption of quantum security.**
- Currently no viable commercial applications of QC and not expected in the next five years.

PROMINENT PLAYERS

- D-Wave model is very different to that of Google or IBM. Is focused on optimization problems and will probably never be able to solve Quantum Mechanics related problems.
- **No one exactly knows what the D-Wave's 2000 qubits QC is**
- NA is forefront of QC R&D, Europe follows and APAC currently behind. APAC QC hubs are Japan, China, Australia, Singapore.
- IBM's top QC startups: Zapata Computing, Strangeworks, QxBranch, Quantum Benchmark, QC Ware, Q-CTRL, Cambridge Quantum Computing (CQC), 1QBit – Link
- **After Chinese govt. announced USD +10bn investments in QC hardware, Chinese software players are also investing heavily, focusing on SW (e.g. Alibaba USD +15bn)**

16. Case Study: QC Software Startup- QxBranch

Company Description

- Spinoff from Aerospace Concepts, another Quantum Computing venture
- Develops and tests commercial applications for quantum computing. It is betting on the computer power of QC to develop solutions for optimization problems and use Machine learning for AI.
- HQ is in Washington, D.C., with offices in Hong Kong, London, and Adelaide, Australia.

Focus

- Wide range of advanced analytics problems and is recently partnering and making some significant progress with financial institutions.
- Unique approach: it is trying to develop advanced analytics solutions simulating a QC environment and, in words of Michael Brett, its CEO, when true QC power becomes available *"we just swap out our simulation for the real hardware."*

Team Profile

- Multi-disciplinary team including systems engineers, computer scientists, mathematicians, quantum physicists, and economists.
- Michael Brett, CEO, who came to found QxBranch from a COO position in Aerospace Concepts, QxBranch parent
- Roy Johnson, chairman, who served as CTO of Lockheed Martin and who led that company to purchase the first Quantum Computer outside the public sector from D-Wave

Funding and recognition

- Raised a total of $5.5M so far in Seed and Series A funding
- Selected by IBM, one of the leaders in QC Hardware development, among only other eight startups, to partner for the development of the first QC based applications.

Source: CEO interview and secondary Research