Quantum Computing

Professor Lloyd Hollenberg

IBM Q Hub @ The University of Melbourne,

ARC Centre for Quantum Computation & Communication Technology

CHEP2019, Nov 7 2019

Outline

Introduction – quantum logic and information processing

Quantum search 101 – the QUI system

Quantum error correction and scale-up

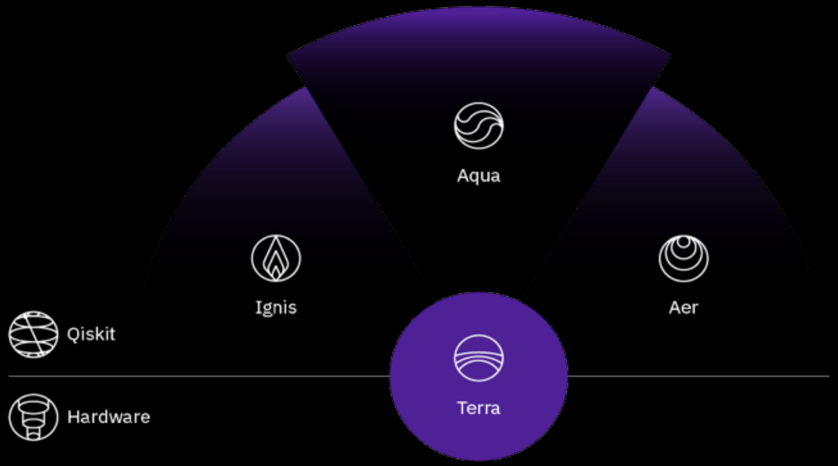
Quantum factoring, HPC simulations

Emerging quantum computers, “supremacy”

IBM Q Hub @ UoM – research highlights

Quantum computing and HEP

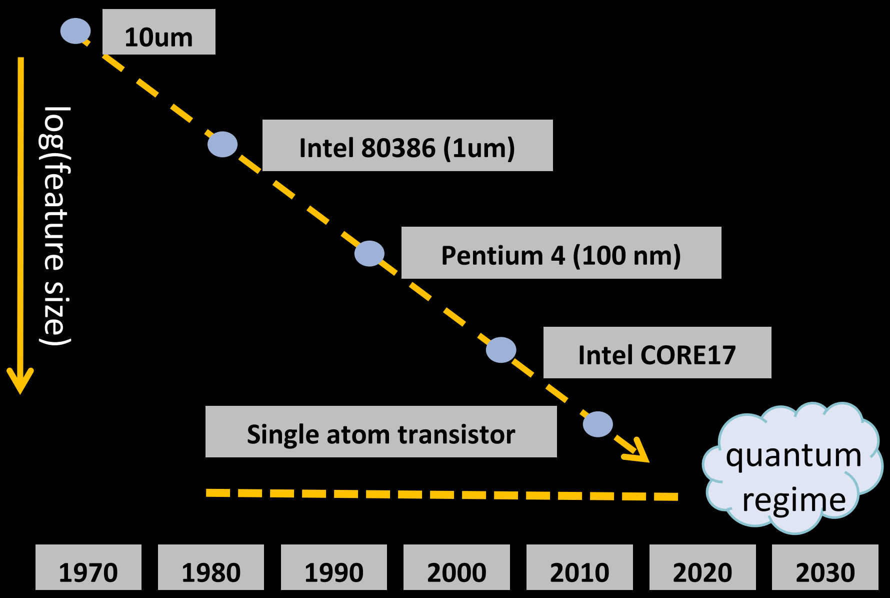
QUIspace.org



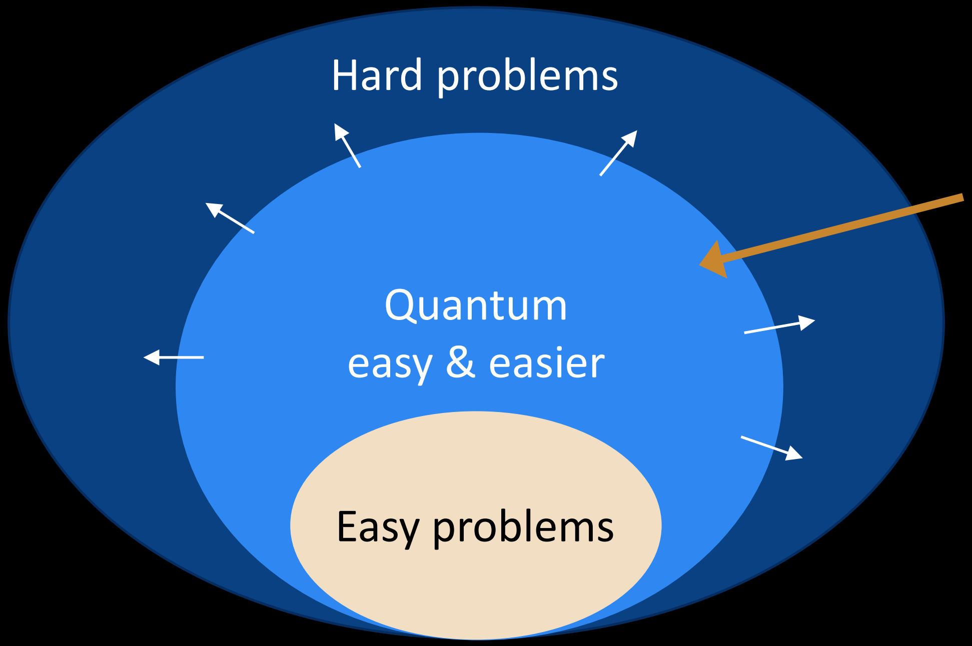
IBM.com

Quantum computing: drivers

Hard problems: generally scale poorly with (classical) CPU resources, technology plateau (Moore's Law final gasp)



Conventional transistor miniaturization
…the end of Moore's Law is nigh



space of quantum apps being explored

e.g. optimisation, finance, AI, materials…

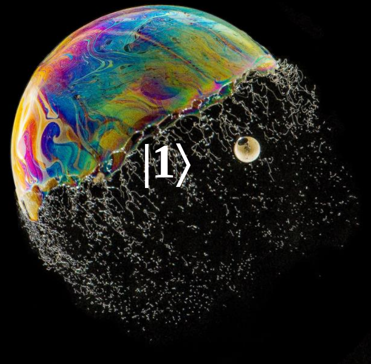
Quantum computers based on the laws of quantum mechanics circumvent limitations of classical information processing

Bubble: commons.wikimedia.org
Bursting bubble: williamhortonphotography.com

Quantum information…the important bits

Quantum superposition – multiple possibilities existing at the same time

Quantum measurement – collapse to one possibility when ”observed”



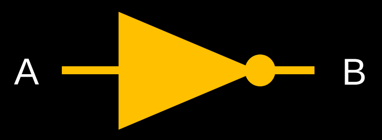
Quantum entanglement – observation of one part affects another part

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Quantum logic

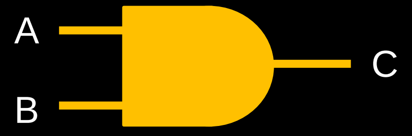
Classical logic: bit by bit

Classical NOT gate



A	B
0	1
1	0

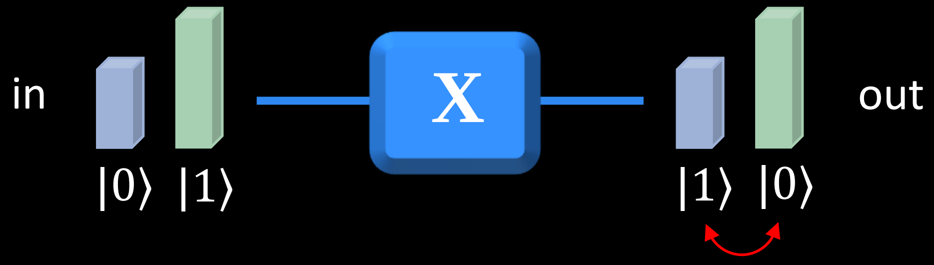
Classical AND gate



A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

Quantum logic

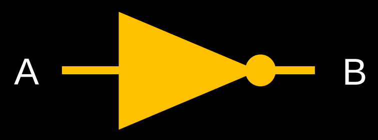
Quantum NOT gate $\rightarrow$ both bits flipped at <u>same time</u>



Quantum logic

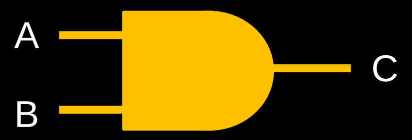
Classical logic: bit by bit

Classical NOT gate



A	B
0	1
1	0

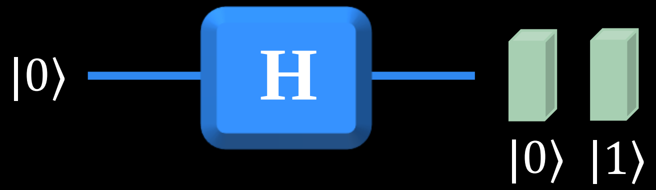
Classical AND gate



A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

Quantum logic

Quantum Hadamard gate → create superpositions

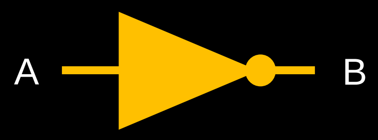


Quantum Controlled-NOT: all 2-bit strings at same time

Quantum logic

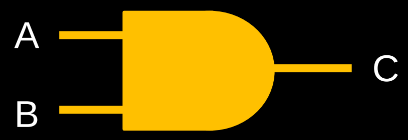
Classical logic: bit by bit

Classical NOT gate



A	B
0	1
1	0

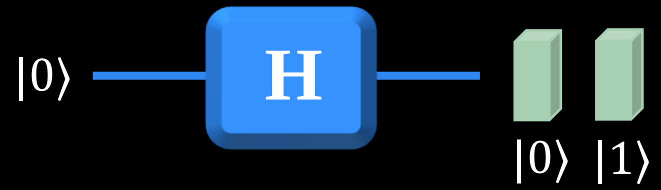
Classical AND gate



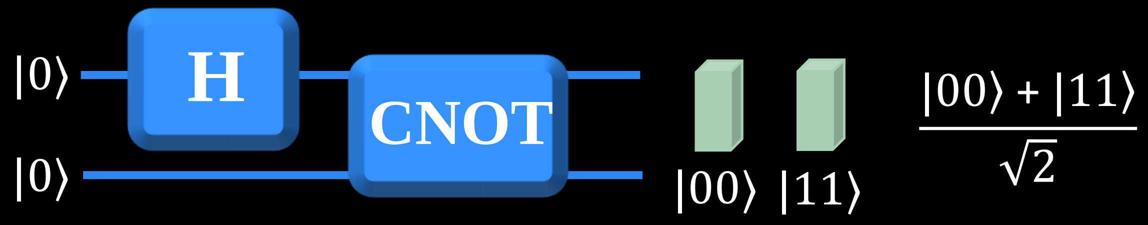
A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

Quantum logic

Quantum Hadamard gate → create superpositions



Quantum Controlled-NOT: all 2-bit strings at same time

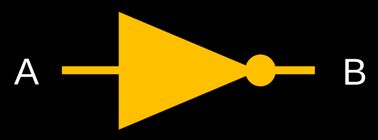


Quantum gates in combination create generalized superpositions → entanglement

Quantum logic

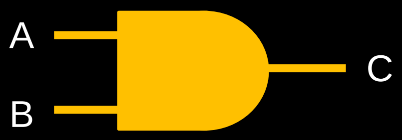
Classical logic: bit by bit

Classical NOT gate



A	B
0	1
1	0

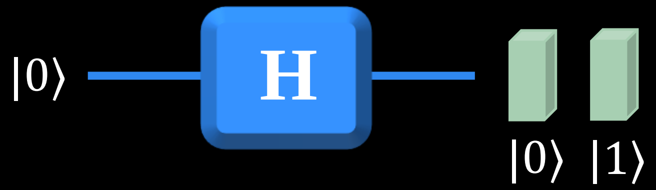
Classical AND gate



A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

Quantum logic

Quantum Hadamard gate → create superpositions



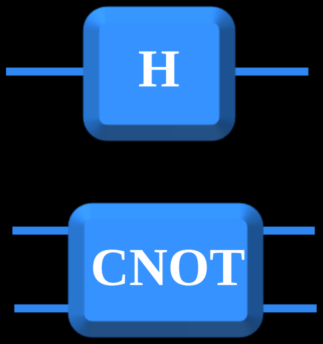
Quantum Controlled-NOT: all 2-bit strings at same time

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

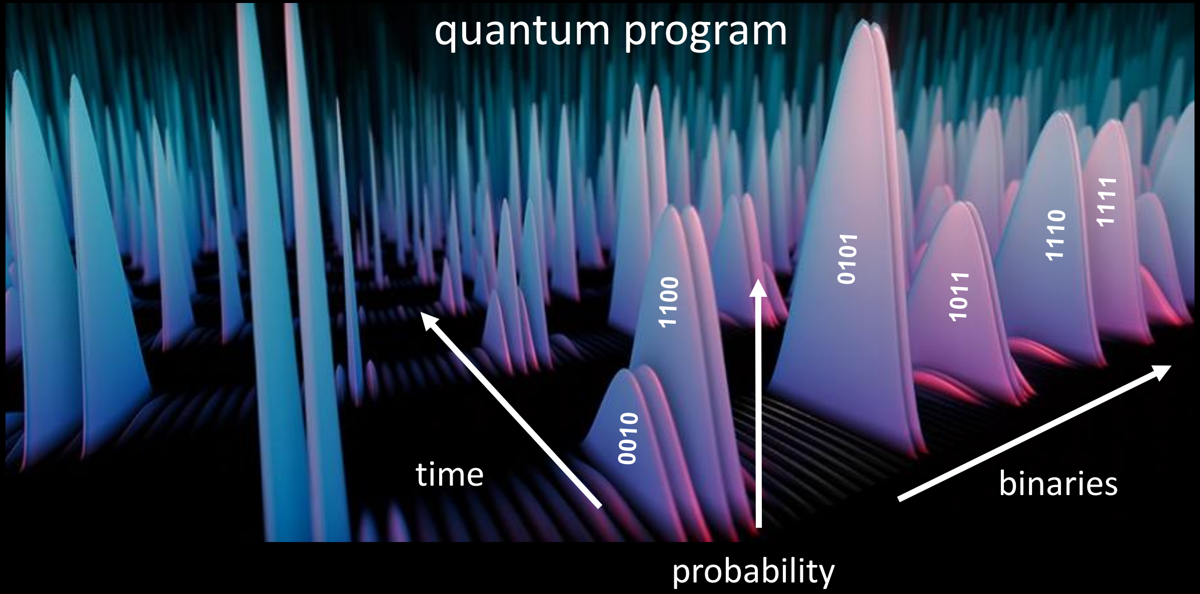
Quantum gates in combination create generalized superpositions → entanglement

Quantum information processing

- logic gates between qubits perform mathematical operations on binary data
- complex entangled states created → binary data are quantum "linked"
- quantum interference amplifies probability of desired output (answer)



start



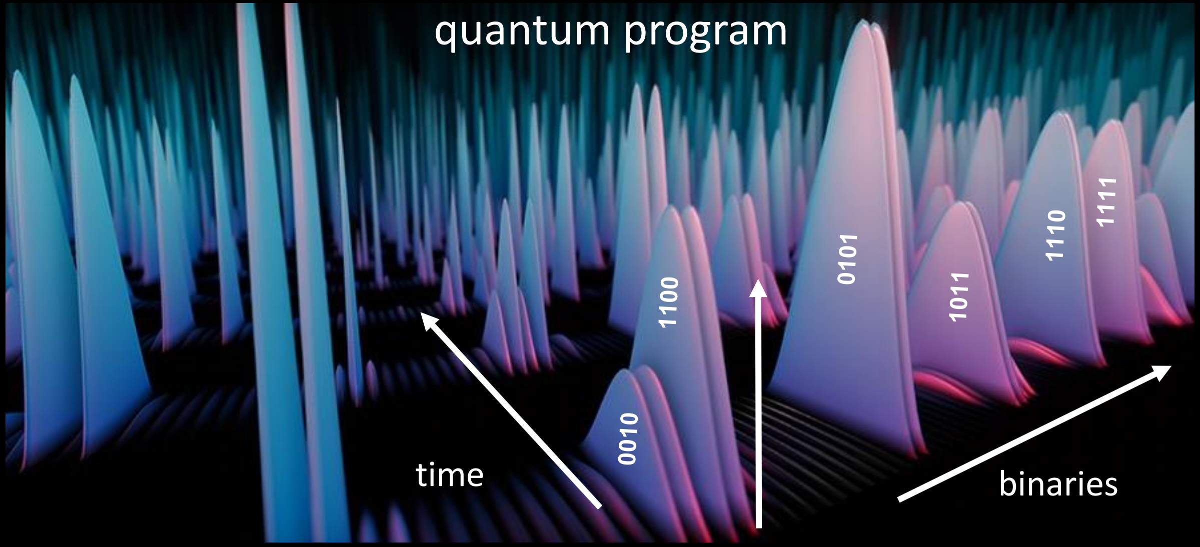
finish

THE UNIVERSITY OF MELBOURNE

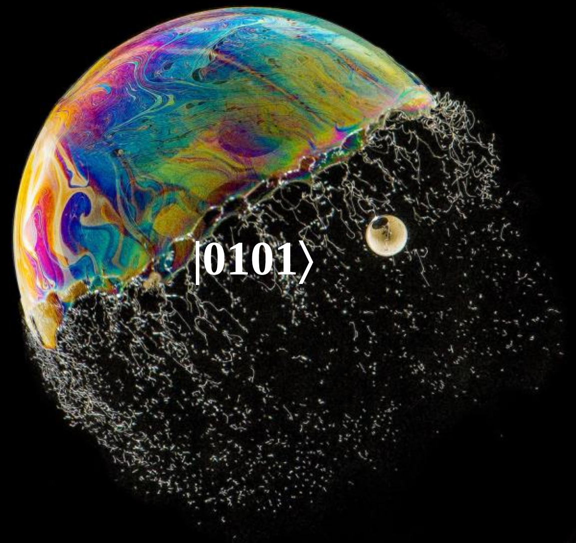
Quantum information processing

- logic gates between qubits perform mathematical operations on binary data
- complex entangled states created → binary data are quantum "linked"
- quantum interference amplifies probability of desired output (answer)

quantum superposition

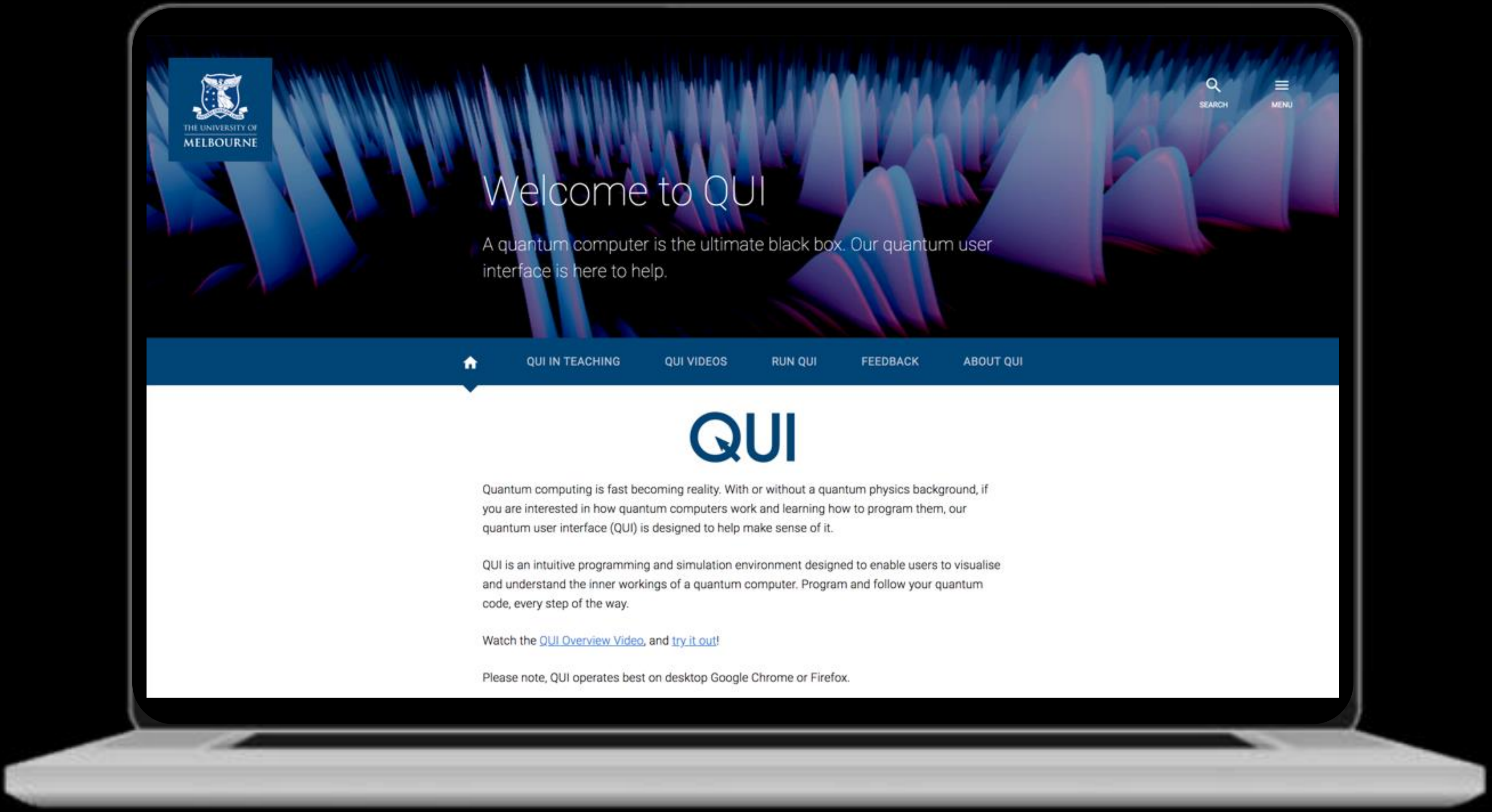


probability



read-out

UoM: Quantum User Interface (QUI)



UoM
QC programming
and simulation
environment
for teaching,
research, outreach

quispace.org

UoM: Quantum User Interface (QUI)

UoM
QC programming
and simulation
environment
for teaching,
research, outreach

quispace.org

Quantum search 101 – needle in a haystack

Problem: alphabetical phone book, given a number find the name…

Classical: N entries $\rightarrow$ on average $\sim N/2$ tries (look-ups).

Quantum: Quantum search ("Grover's algorithm") $\sim\sqrt{N}$ tries

Example: imagine our data-base (the phone book) is all eight 3-bit numbers $\rightarrow$ search on one entry (say the number 5 = 101)

"Database" in superposition:

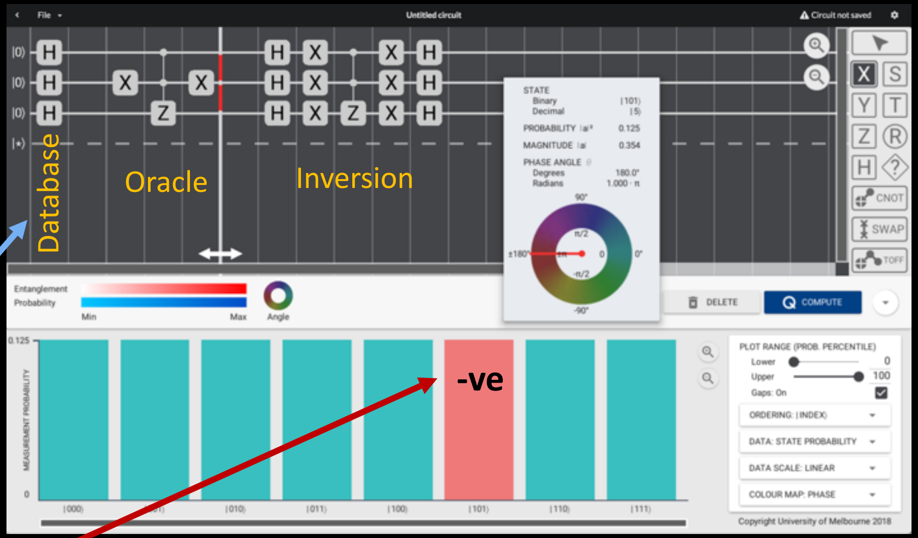
$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

"Oracle" marks 101 state:

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle - |101\rangle + |110\rangle + |111\rangle)$$

"Inversion" amplifies probability of the marked 101 state.

Quantum search algorithm manipulates the amplitudes so that the probability of the result is amplified – i.e. magnifies the needle…



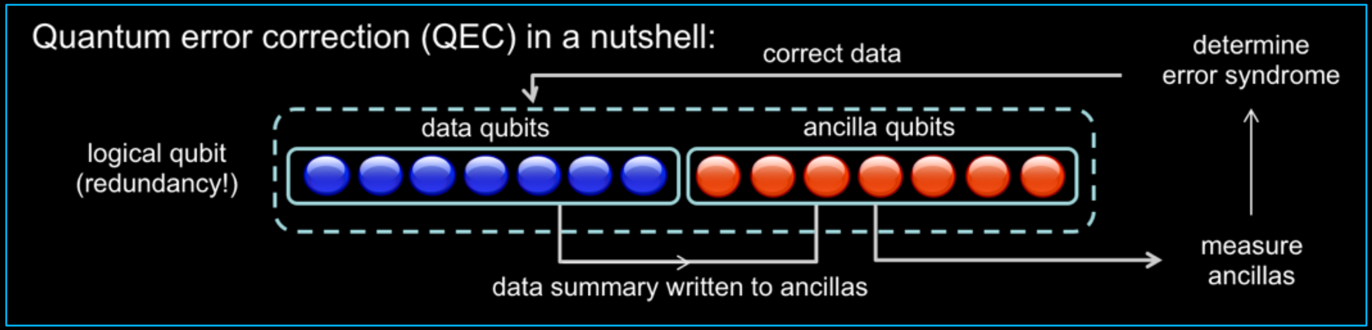
Quantum error correction and scale-up

Quantum logic is extremely vulnerable to decoherence and control errors…

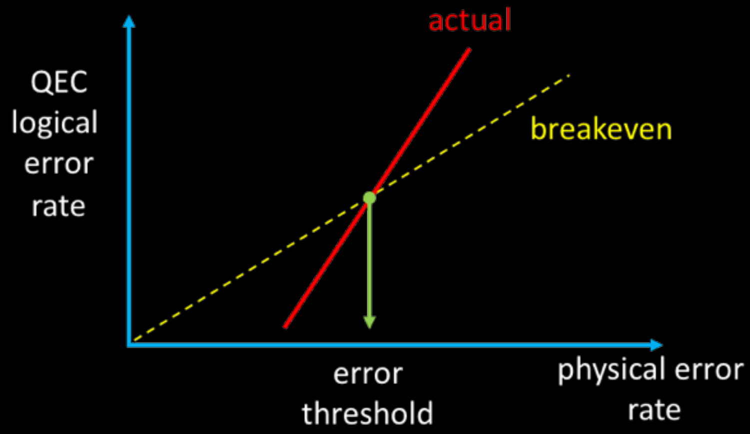
Essential dilemma:

How do you correct if measurement collapses state?

Quantum Error Correction!



Redundancy & gates → more errors
→ error threshold



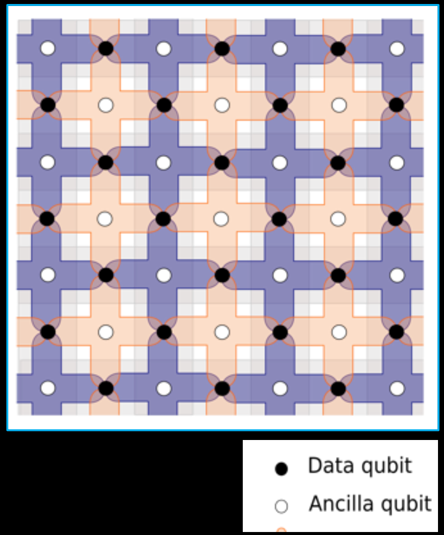
Topological QEC on 2D array (surface code)

Kitaev 1997, Raussendorf/Harrington 2007

Threshold >1% (Wang et al 2011)

TQEC is a game changer, but still 1000’s of physical qubits per logical qubit

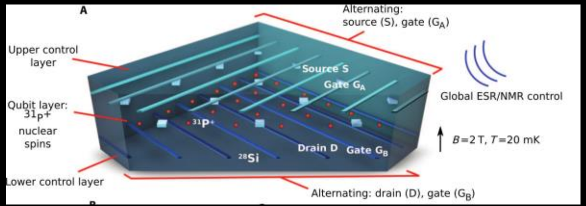
logical qubit



1D: QEC threshold ~10^{-7} (Skopek 2007)

2D: QEC threshold ~10^{-5} (Svore et al 2005)

2D architectures:
(e.g. Hill, LH et al Sci Adv. 2015)



Quantum factoring algorithm (Shor)

The quintessential example:
semi-prime factoring…

hard ←

$p \times q = N$

→ easy

Kleinjung et al (2009): RSA768
1,500 core-yrs

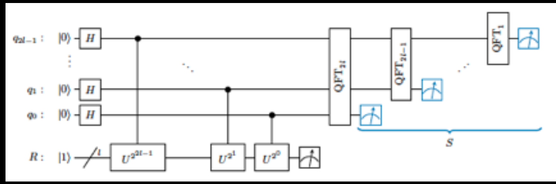
N[RSA-768] = 1230186684530117755130494958384962720772853569595334792197
3224521517264005072636575187452021997864693899564749427740
6384592519255732630345373154826850791702612214291346167042
921431160222124047927473779408066535141959745985690214341 3 = p x q

p = 3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9

q = 3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

Digicert (SSL): to crack 2048 bit key → (>>age of Universe) core-yrs

Shor's quantum factoring algorithm → "quantum easy"



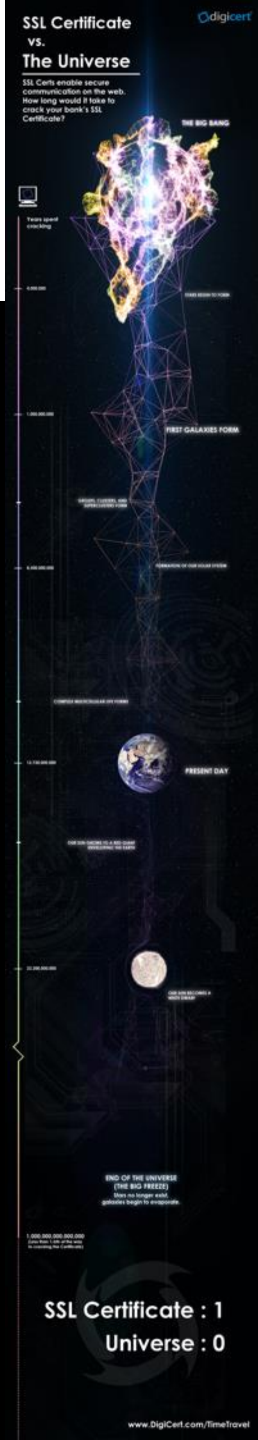
QC: 2048 bit case → thousands of logical qubits (& QEC) → c. 10m physical qubits

Quantum Advantage: some years before QC outperforms HPC on RSA problems…meanwhile:

<u>Post-quantum Cryptography</u>

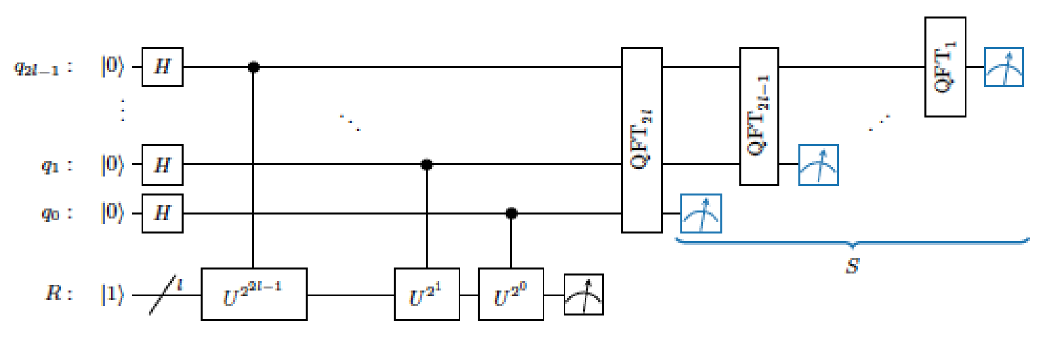
Impact of <u>full-scale</u> QC on current and future crypto-systems (e.g. RSA) → high

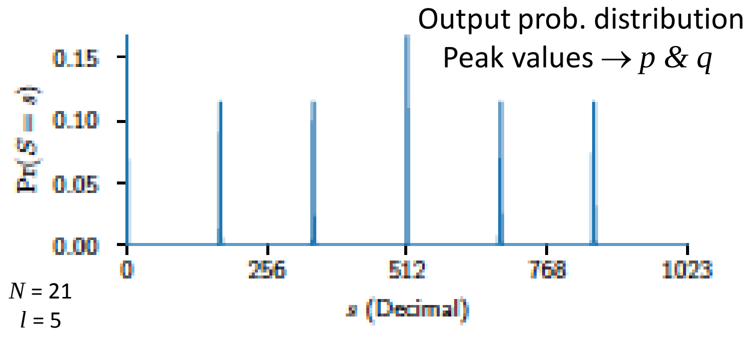
→ NIST Post-Quantum Cryptography Standardization project



Classical simulations of quantum circuits

Shor's quantum factoring algorithm for a l-bit semi-prime, $N = p \times q$:



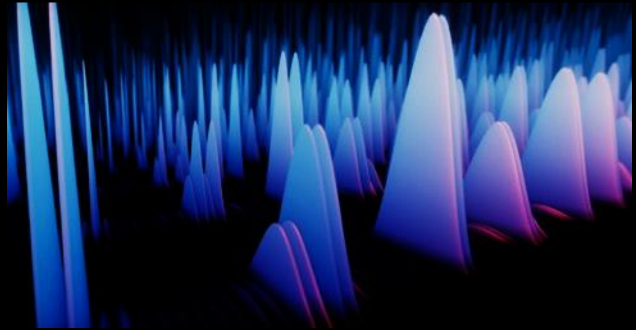


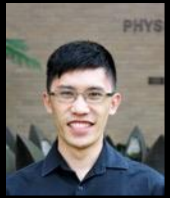
Challenge: sample from the distribution $P(s)$ by simulating $3l$ qubit circuit output

Hilbert space dimension: $3l$ qubits → 2^{3l} complex amplitudes (i.e. 2^{3l} x 2 x 8 bytes)

Our method: Matrix Product State (MPS)…storage ~ entanglement

- Simulated up to **60 qubits**: N = 961,307, l = 20
- MPS actual: 5184 cores, 13.8 TB, 8h (Pawsey HPC Centre)





Aidan Dang et al
Quantum 3 116 (2019)

NB: Full Hilbert space for 60 qubits: 18 exabytes → Shor's algorithm is very frugal with entanglement…

HPC 2018 READERS' CHOICE AWARDS Cast your Ballot!

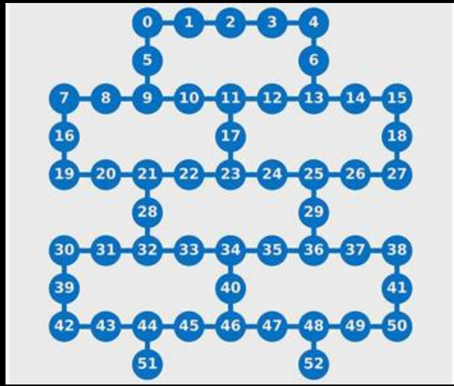
Meanwhile: quantum computers emerge

2016: IBM provides cloud access to QC hardware, programming interface

2017: IBM Network Q

Major players: Rigetti, Google, IonQ, Microsoft, Intel, D-Wave,…

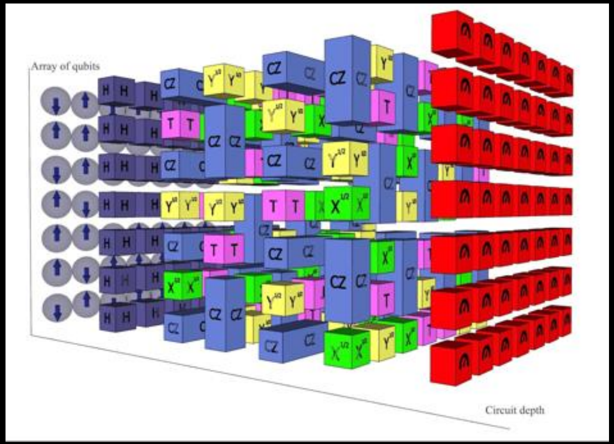
IBM.com



2019: “System One” IBM state-of-the-art

Stand-alone QC systems (20 $\rightarrow$ 53 qubits), fully programmable

Nov 5 2019: Qiskit software stack supports access to AQT ion-trap QC



Google.com: quantum circuit sampler machine

“Quantum supremacy”

$\rightarrow$ 54-1 qubits beat HPC for simulating QC circuits (Google)
$\rightarrow$ 200 sec (QC) v s. 10,000 yrs (HPC) [Nature Oct 23 2019]

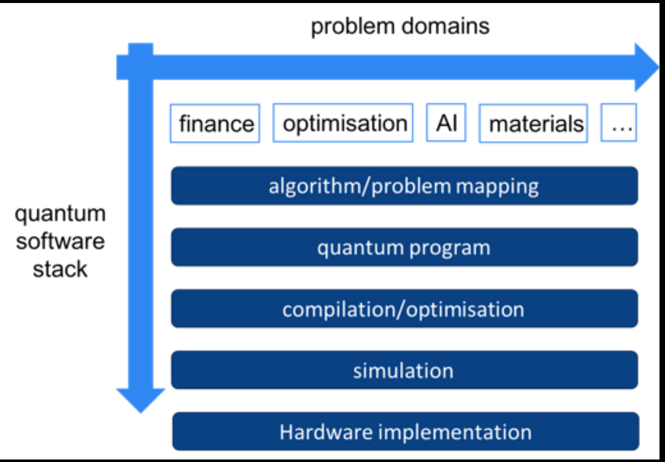
IBM: more like 2.5 days on HPC [arXiv:1910.09534]

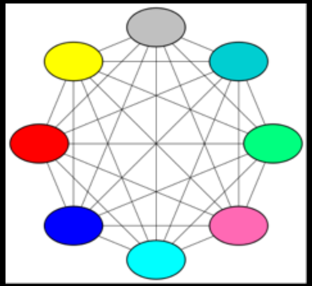
Big goal: “Quantum advantage”

$\rightarrow$ beat HPC on a <u>useful</u> problem (if/when?)

Quantum algorithms and applications: NISQ era

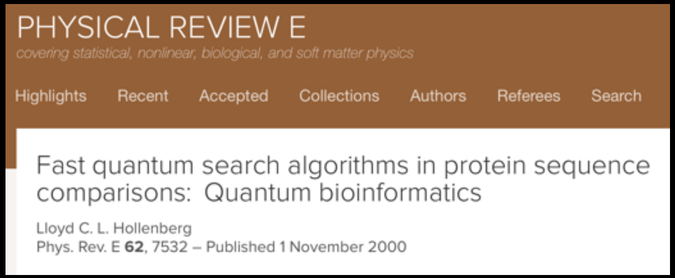
Quantum algorithms exist for for a range of problems: optimisation, sampling, system simulation…





New era, old strategy: adapt quantum algorithm to purpose…

e.g. quantum search algorithm → bioinformatics (2000)



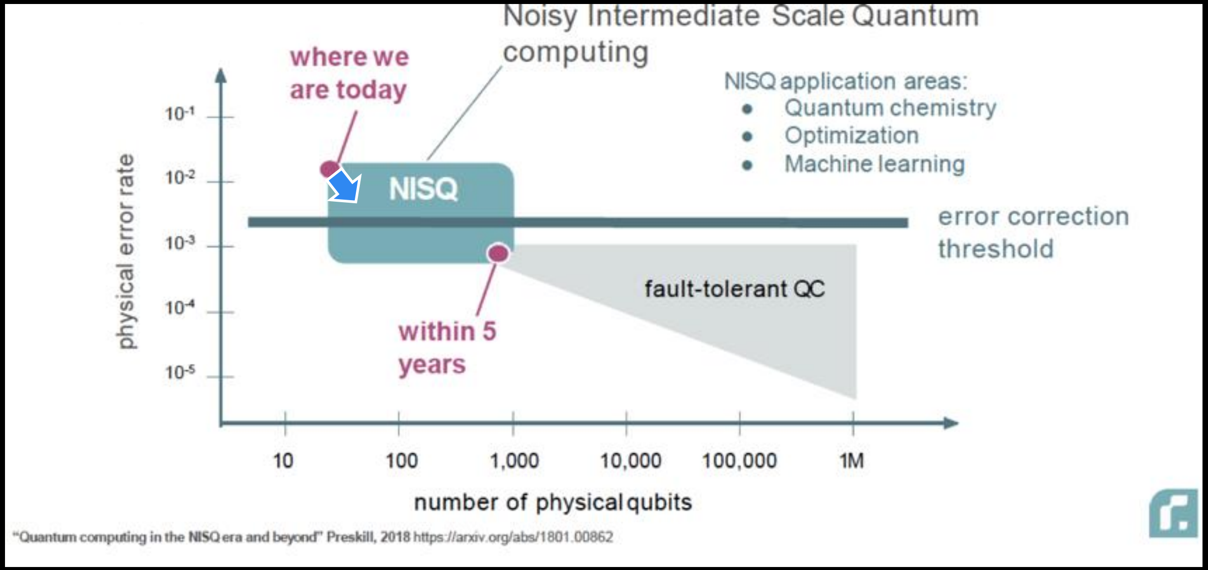
PHYSICAL REVIEW E
covering statistical, nonlinear, biological, and soft matter physics

Highlights Recent Accepted Collections Authors Referees Search

Fast quantum search algorithms in protein sequence comparisons: Quantum bioinformatics

Lloyd C. L. Hollenberg
Phys. Rev. E **62**, 7532 – Published 1 November 2000

NISQ: Noisy Intermediate Scale Quantum (Preskill)



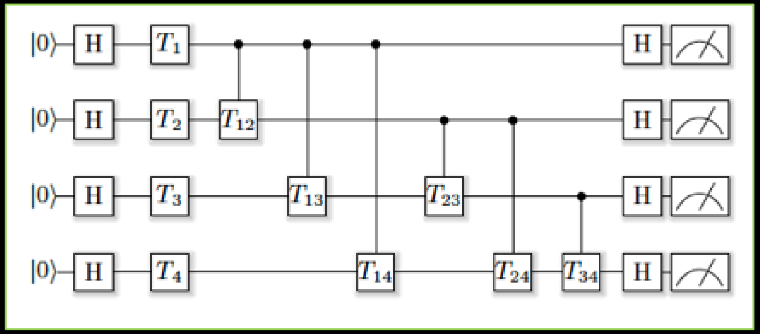
Key question: quantum advantage in NISQ era?

NISQ: instead of "big data", think "big models"…

→ applications in HEP…

Effect of quantum logic gate errors: simulations

Instantaneous Quantum Polynomial circuits:



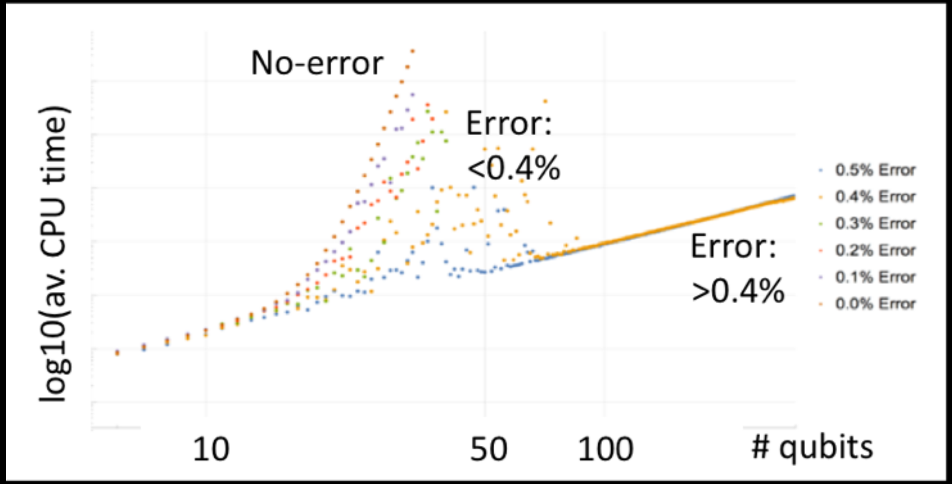
Determine output prob. distribution

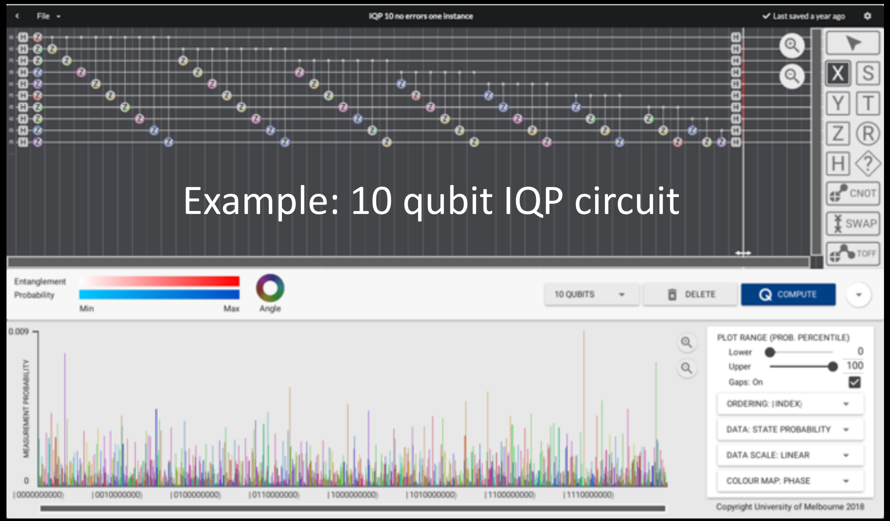
Semi-random phase gates

$$T_m = \exp\left(i\frac{k_m\pi}{8}Z_m\right)$$

$$T_{mn} = \exp\left(i\frac{k_{mn}\pi}{8}Z_m Z_n\right)$$

C. Hill,
M. Bremner, LH
2018/19





MPS simulations (Pawsey Supercomputer Centre)

(Z-errors, qubit reduction technique)

Results: evidence for cross-over at ~ 0.4% gate error rate

Specific to IQP, but possibly indicative for phase intensive calculations

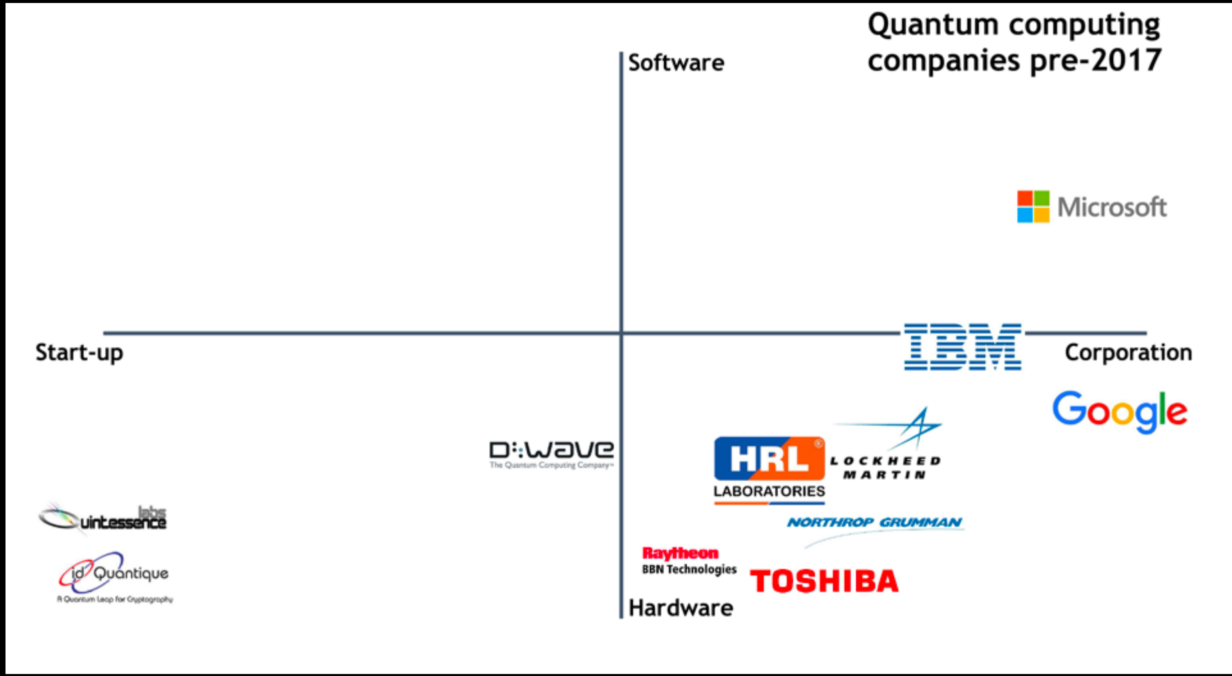
(and close to where hardware is at…)

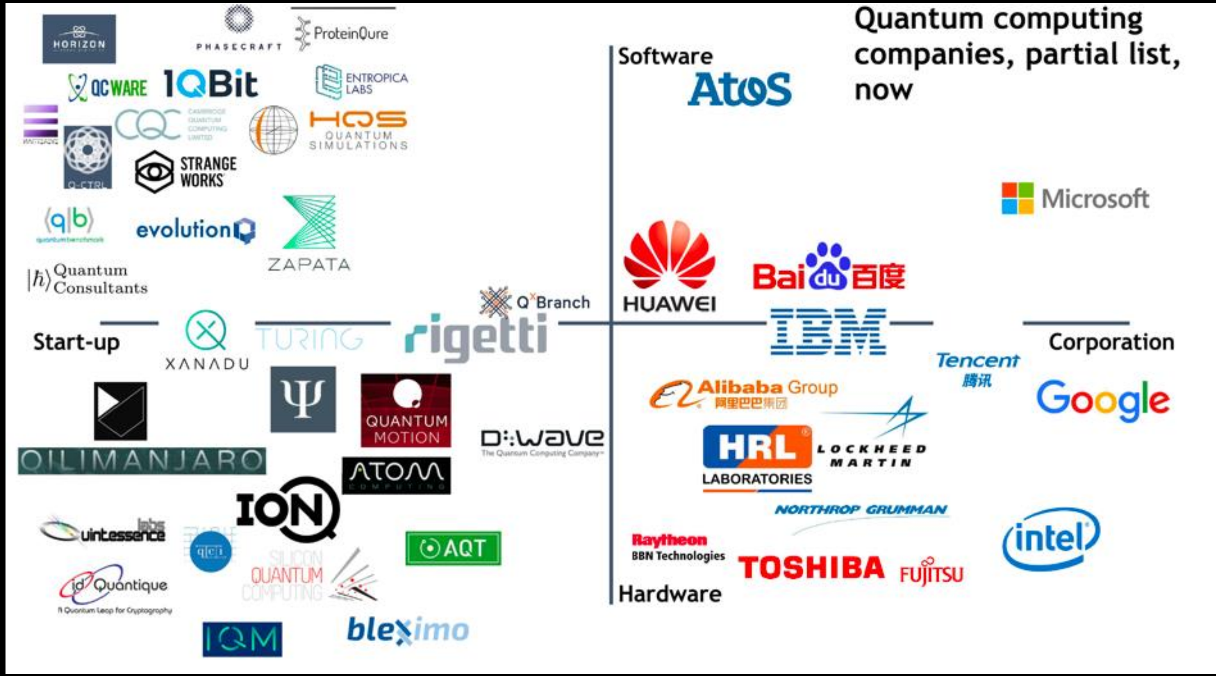
How fast are things moving?

Quantum computing literature:

Journal club – no longer 1-2 papers/week, now deal with c.50 new/interesting abstracts per week…

Start-up status: pre-2017 and present (courtesy S. Devitt)





The IBM Q Network launched in Dec 2017…

Accelerate Research

Launch Commercial Applications

Educate and Prepare

IBM Q Network

77 members

- 7 industry partners
- 9 hubs
- 16 members
- 19 startups
- 26 academic partners

Industry Partners	Hubs	Members	Startups	Academic Partners
ExxonMobil	Oak Ridge National Laboratory	Barclays	QC Ware	MIT
JP Morgan Chase & Co.	Keio University	Mizuho	Grid	EDX.org
Samsung	NC State University	MUFG	Quemix	Virginia Tech
Daimler	The University of Melbourne	Mitsubishi Chemical	CQC	U. Montpellier
JSR Corporation	University of Oxford	Argonne Lab	1QBit	Notre Dame
Accenture	University of Bundeswehr Munich	Fermilab	Zapata	Harvard
US Air Force Research Lab	National Taiwan University	Berkeley Lab	Strange Works	Princeton
	University of Minho	Brookhaven Lab	Q-CTRL	Florida State
	CSIC Spain	ITRI	Quantum Benchmark	U. Stony Brook
		III Taiwan	MDR	U. Chicago
		CERN	Qu&Co	U. Tokyo
		Iberian Nanotechnology Laboratory	JoS Quantum	Duke
		Honda	SolidStateAI	UC Boulder
		Hitachi Metals	ProteinQure	U. Waterloo
		Nagase	Labber Quantum	U. Illinois
			MaxKelsen	Northwestern
			Netramark	NYU
			Entropica	Wits
			Boxcat	Aalto University
			Rahko	U. of Turku
				U. Basque Country
				U. of Innsbruck
				EPFL
				Chalmers University
				ETH Zurich
				Saarland University

THE UNIVERSITY OF MELBOURNE

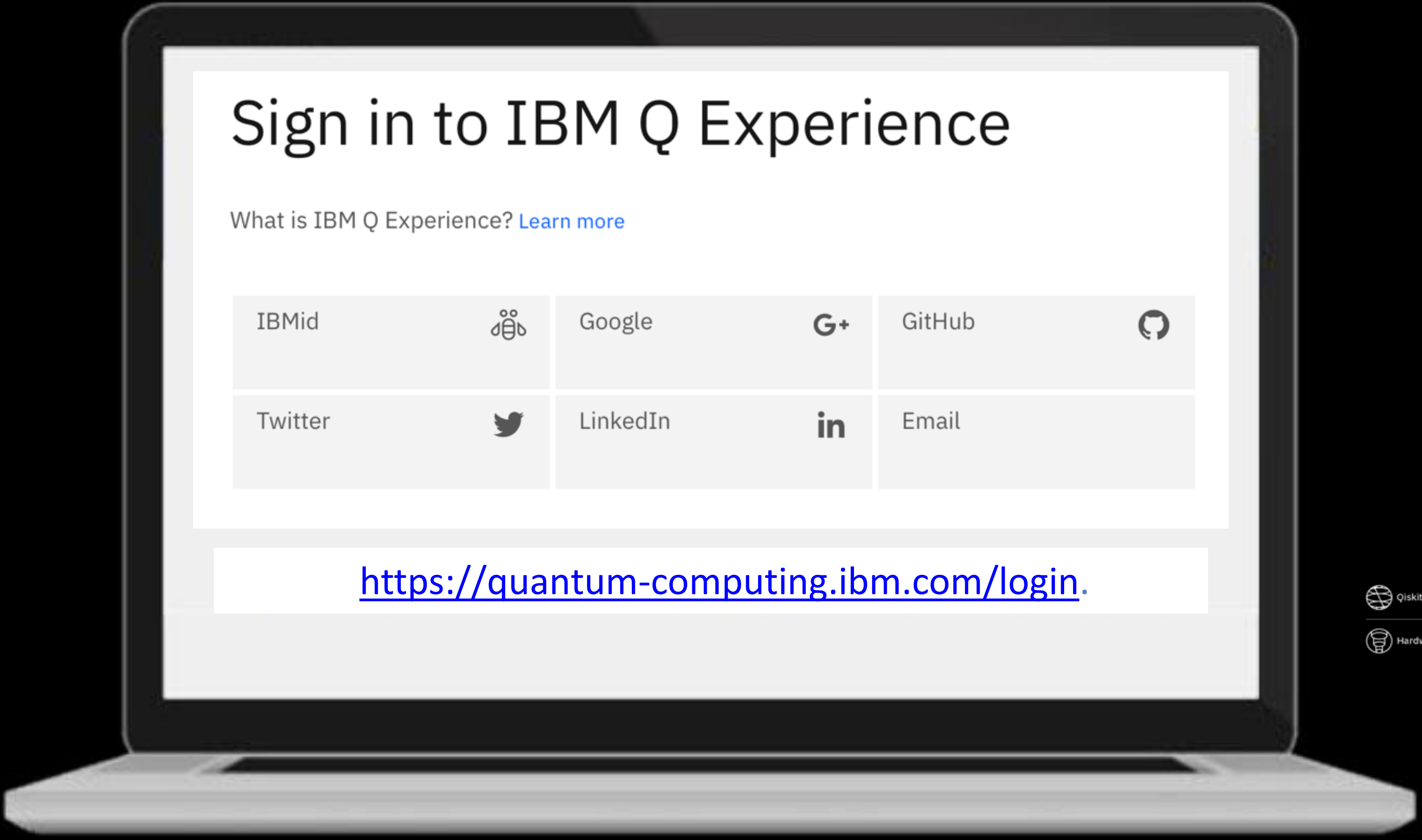
Australian IBM Q Hub

- Industry engagement
- Research
- Education
- Outreach
- Premium IBM QC

IBM.com

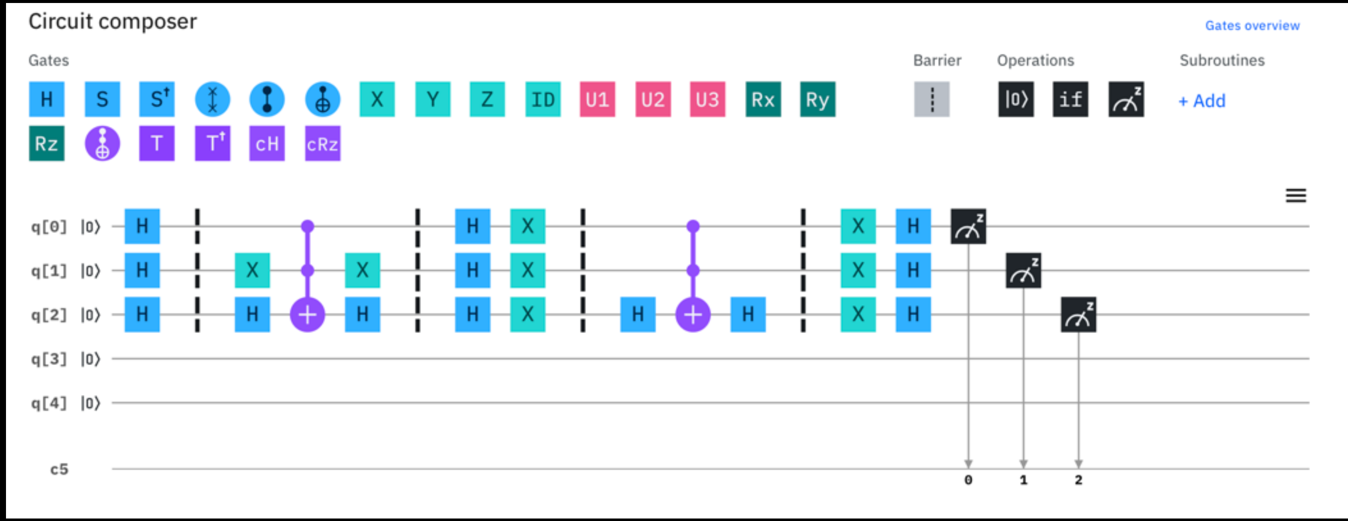
research.unimelb.edu.au/QuantumHub

IBM Quantum Experience

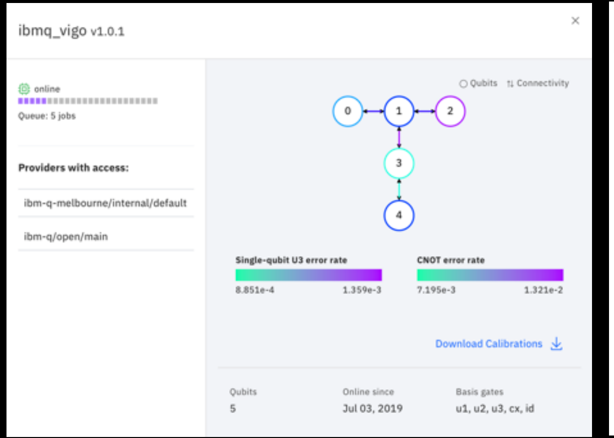


https://quantum-computing.ibm.com/login.

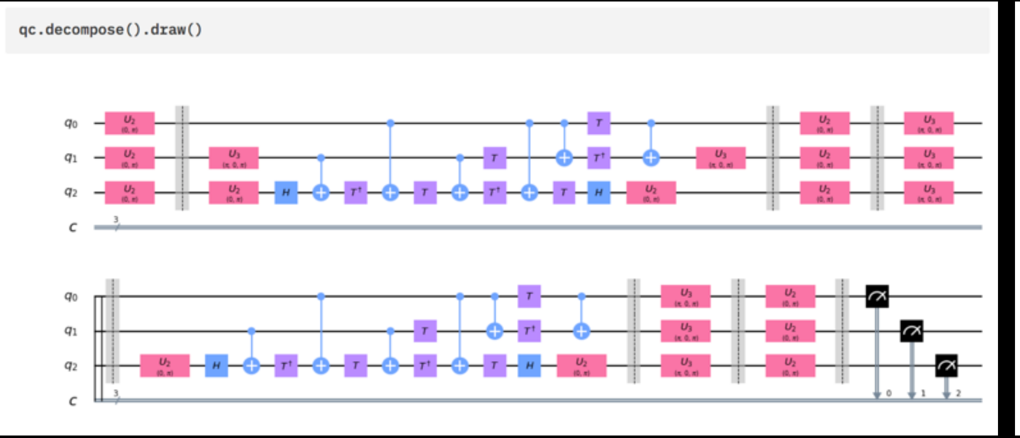
Quantum search 101 on IBM Q



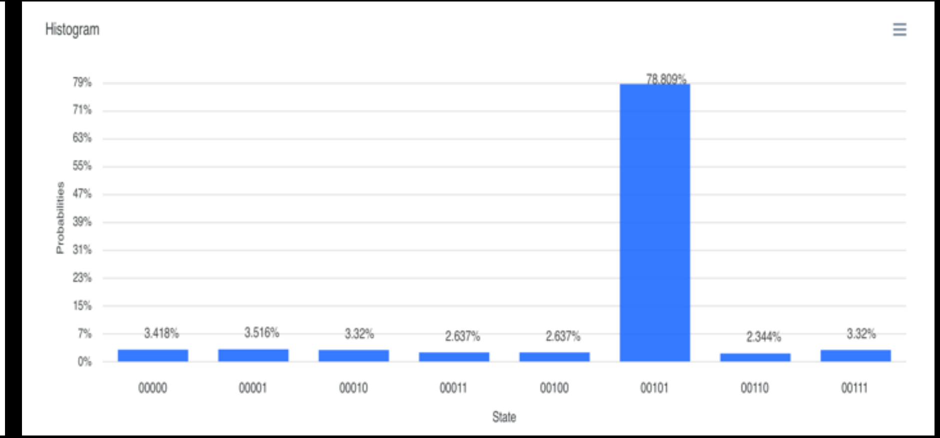
Pick a backend (vigo = open)



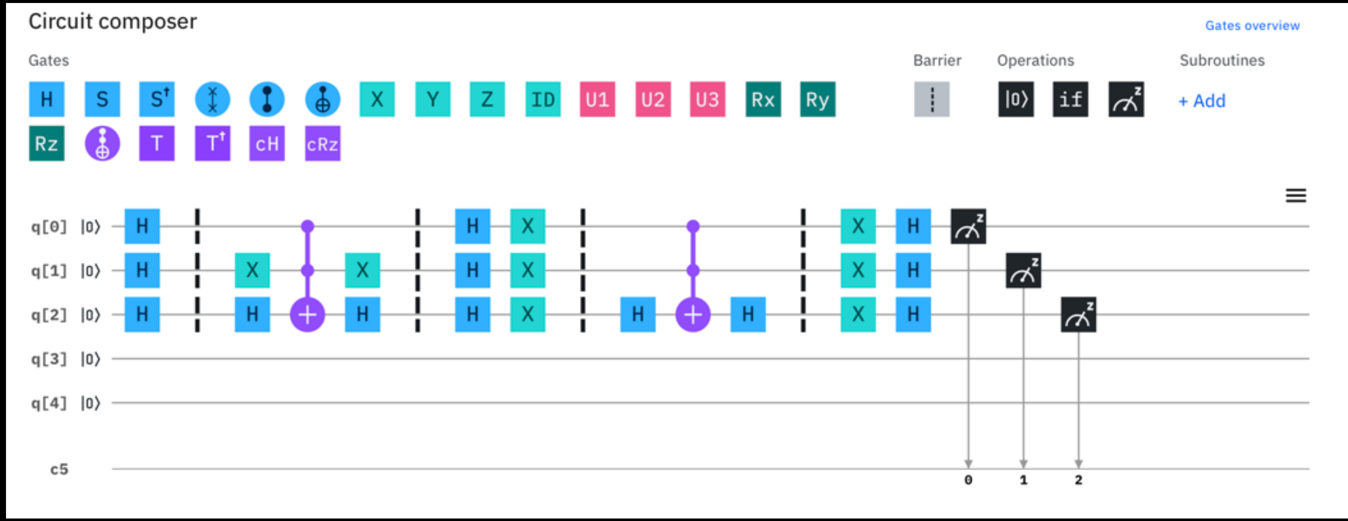
Actually runs this circuit…



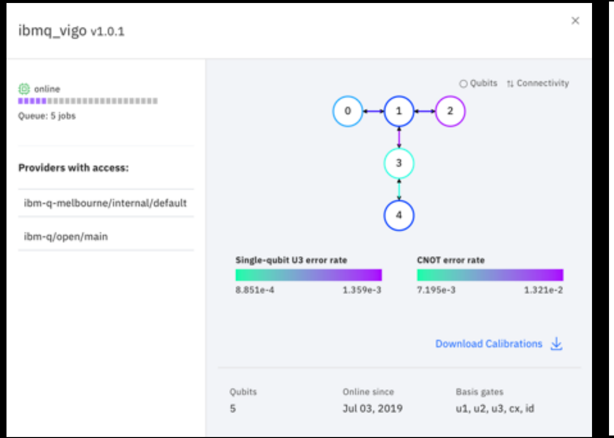
Results – QASM simulator



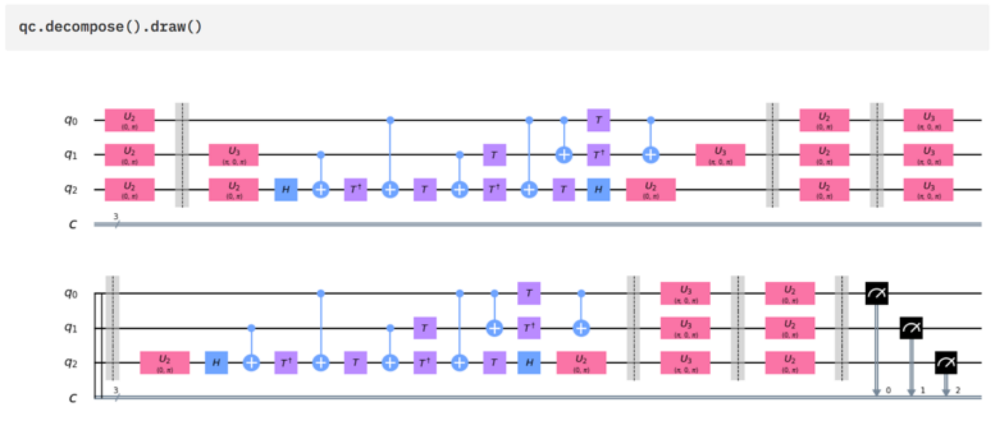
Quantum search 101 on IBM Q



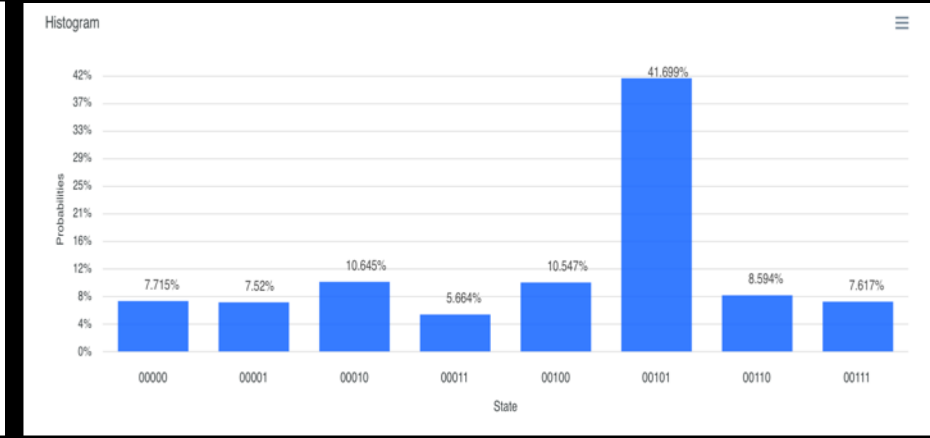
Pick a backend (vigo = open)



Actually runs this circuit…



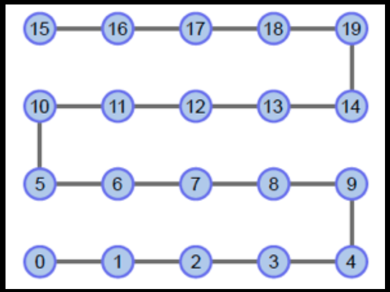
Results – Vigo

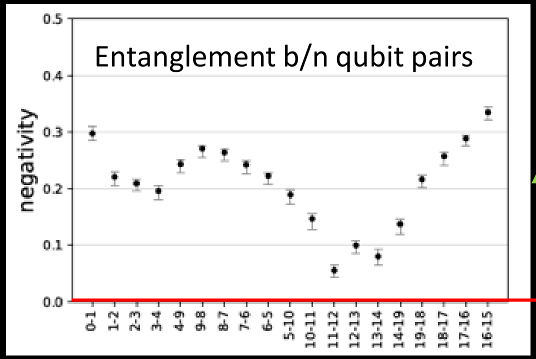


Research at UoM Q Hub: highlights (2018/19)

Gary Mooney (PhD) et al:

Entangled 20 qubit graph state on IBM Q (GM et al, Sci Rep 2019)





entangled

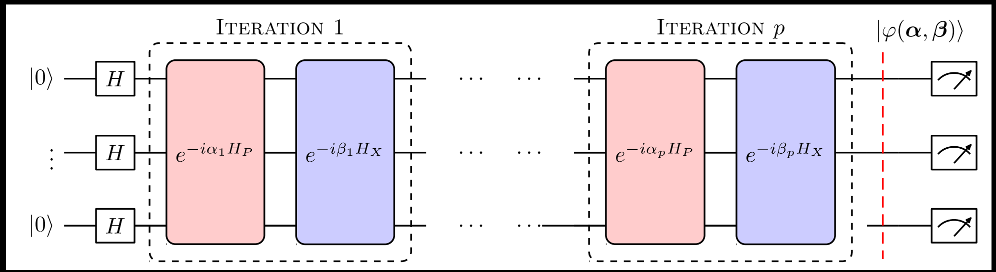
separable

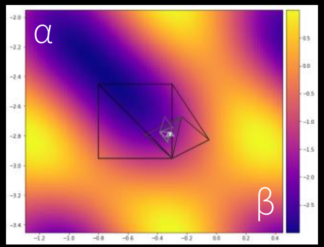
Sam Tonetto (PhD) et al:

Semi-prime factoring via QAOA on IBM Q

cost fn = bitwise(N-p.q)^2

-> some problem reduction shortcuts…



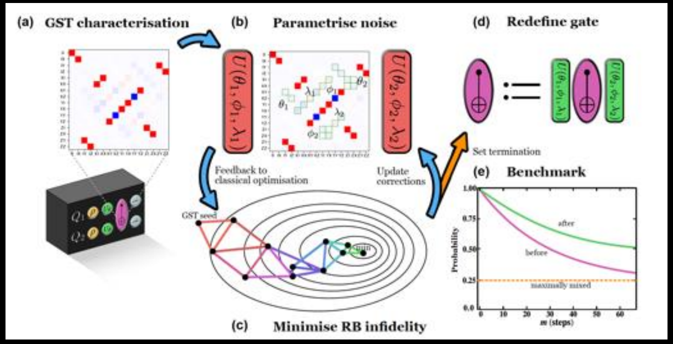


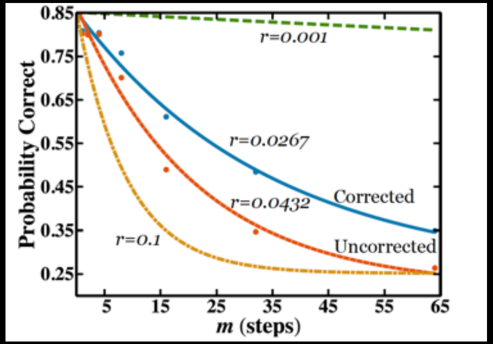
17,812,997 = **4,159 x 4,283**

Greg White (PhD) et al:

Procedure to improve CNOT gate

-> demonstrated fidelity increase on IBMQ [-> Nov arXiv]



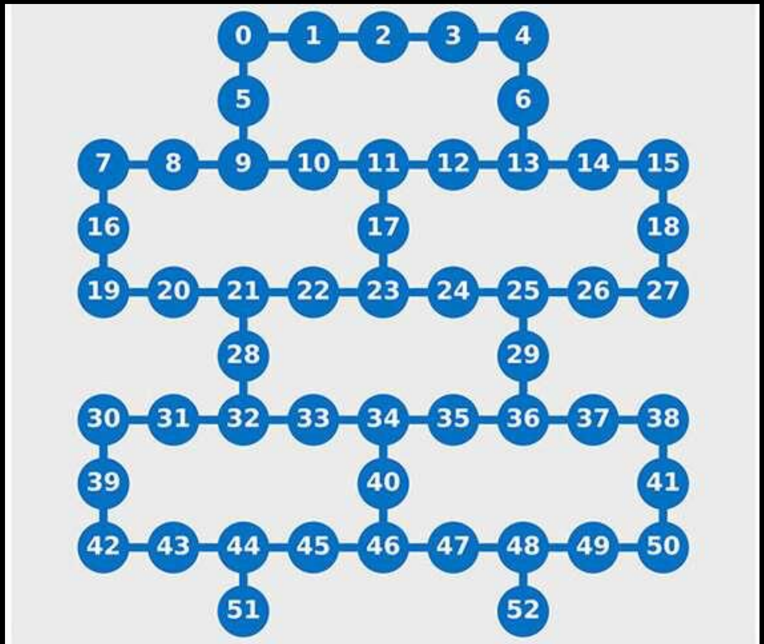


Demonstrated on IBM Q

-> randomised benchmarking

CNOT optimisation across multiple IBM Q calibrations (weeks)

Larger systems – scaling up NISQ



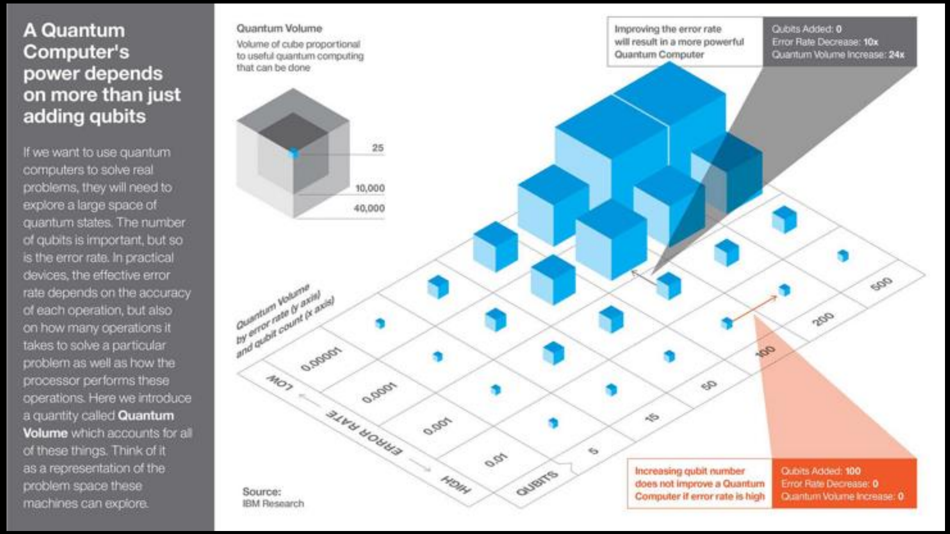
IBM Q 53 qubit device
"Rochester"

As they scale the important factors in a quantum computer are:

- Gate errors
- Qubit connectivity
- Number of qubits

Determines the overall length ("depth") of a quantum circuit before the "en-scrambling" of results…

Combined quantitative measure: "quantum volume"



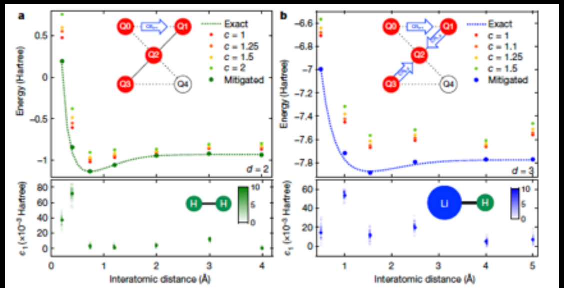
IBM.com

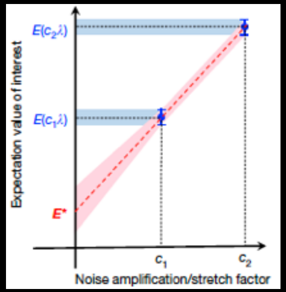
Possibly quantum advantage in specific problems for 100-1000 qubit systems within 5 years…maybe.

Related to HEP…(not exhaustive)

Simulation of quantum systems $\rightarrow$ variational approaches (VQE)

e.g.
$\rightarrow$ chemistry problems (Kandala et al *Nature* 2017)
$\rightarrow$ error mitigation techniques (Kandala et al *Nature* 2018)

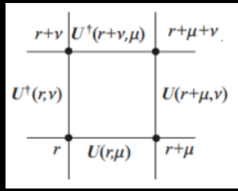


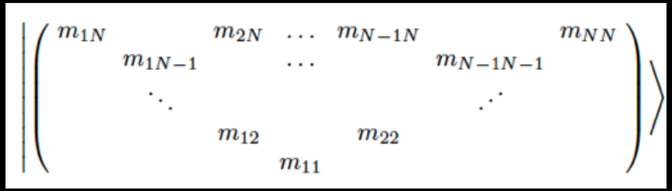


Lattice gauge theory on QC: Byrnes and Yamamoto PRA 2006

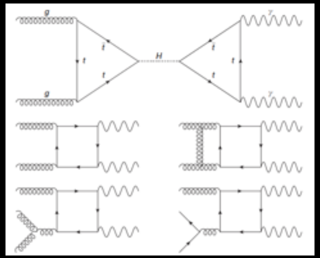
QC and quantum field theory: Jordan, Lee, Preskill 2012-2018
(Review: Preskill *Quantum* 2018, arXiv:1811.10085)

LGT and QC review: Banuls et al arXiv:1911.00003)





QAML: Higgs-signal-versus-background machine learning optimization problem $\rightarrow$ ground state of an Ising spin model (Mott et al, *Nature* 2017)



HEP engagement with QC:
openlab.cern/quantum-computing-high-energy-physics
www.fnal.gov/pub/science/particle-detectors-computing/quantum.html

THE UNIVERSITY OF MELBOURNE

Quantum Information Science and Technology @ UoM

Staff
Lloyd Hollenberg
David Simpson
Charles Hill

Postdocs
Mina Barzegaramiriolya
Nikolai Dontschuk
Liam Hall
Brett Johnson
Jean-Philippe Tetienne
Muhammad Usman

Admin
Rose Cooney
Maureen Luna

Students
David Broadway (PhD)
Alister Chew (MSc)
Aidan Dang (PhD)
Matt Davis (QUI)
Spiro Gicev (MSc)
Robert De Gille (PhD)
Erin Grant (PhD)
Alexander Healey (PhD)
Michael Jones (MSc)
Timothy Kay (MSc)
Scott Lillie (PhD)
Julia McCoey (PhD)
Gary Mooney (PhD)
Viktor Perunicic (PhD)
Sam Scholten (MSc)
Maiyurentheran Srikumar (MSc)
Daniel Sutherland (QUI)
Sam Tonetto (PhD)
Di Wang (MSc)
Greg White (MSc)
Yi Zheng Wong (MSc)
Alex Zable (ME/QUI)

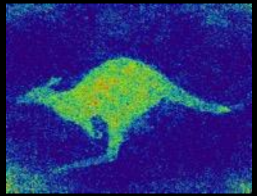
and many collaborators…

Quantum User Interface (QUI)

Quantum computing:

- quantum information
- large-scale architectures
- device simulations
- IBM Q Hub & applications

Quantum sensing:



- new sensing protocols
- quantum hyperpolarisation
- bio-imaging applications
- 2D materials imaging

More information:

Group: blogs.unimelb.edu.au/quantum-technology
UoM research: pursuit.unimelb.edu.au/special_reports
IBM Q Hub @ UoM: research.unimelb.edu.au/QuantumHub
QUI: QUIspace.org
CQC2T: cqc2t.org

Australian Government
Australian Research Council
CENTRE FOR QUANTUM COMPUTATION & COMMUNICATION TECHNOLOGY
AUSTRALIAN RESEARCH COUNCIL CENTRE OF EXCELLENCE