# QEVEC: integrating quantum computing with HPC

**Q**uantum
**E**nhanced
**V**erified
**E**xascale
**C**omputing


Viv Kendon

CNQO
Physics
Strathclyde
viv.kendon@strath.ac.uk


*Manchester – **CIUK 2021** – 9+10 December 2021*


*Funding:* UKRI – EPSRC – ExCALIBUR


*Partners:* UK National Quantum Technologies Programme — QCS Hub (Quantum Computing & Simulation Hub) — NQCC (National Quantum Computing Centre) — CCP-QC

# quantum computing *HYPE*

*'Digital marketing poised for a quantum leap'*

*Quantum Machine Learning — It's time to start now*

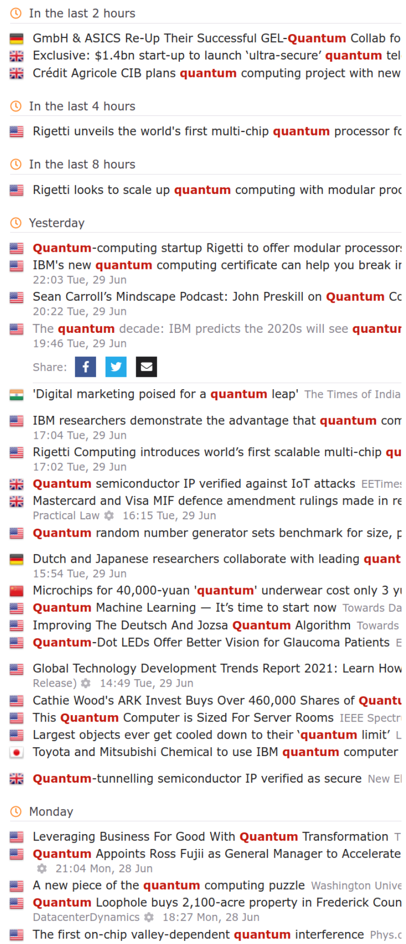
*Microchips for 40,000-yuan 'quantum' underwear cost only 3 yuan . . .*

- wild claims and promises
- talk of revolutions and paradigm shifts
- huge venture capital investment

⟹ *remember:* venture capitalists expect >9/10 to fail

★ this talk: quantum computing without the hype . . .

*headlines from newsnow.co.uk* ⟶



# current quantum computers?

*promises are for venture capitalists . . .* what can they actually do?

- IBM and Google have quantum chips with about 100 qubits
  – *noisy/imperfect even when cooled to very low temperatures*

- running a particular random sampling task (not useful)

- needs **near exascale** classical HPC to verify output

*LOTS of caveats and arguments about this, of course . . .*

$\Longrightarrow$ take home message from the hype:

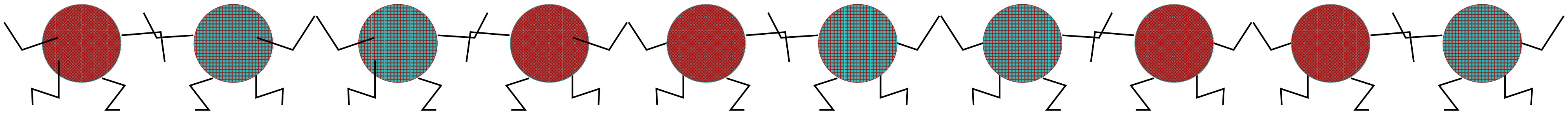
★ potential is real, even for early hardware ★

**★IF★** we can use it for something we actually want to compute . . .

$\Longrightarrow$ time to think seriously about how to use a quantum computer $\Longleftarrow$

# overview of talk

- hype (done)
- co-processors and context
- what is quantum computing?
- how does it work?
- how to make it useful?
- QEVEC and CCP-QC
- opportunities and jobs ...



# hybrid computers . . .

**practice:** co-processors:

*conventional:*

- GPUs graphics cards
- ASIC application-specific integrated circuit
- FPGA field-programmable gate array

*unconventional: control + substrate:*

- quantum
- NMR
- reservoir
- slime mould

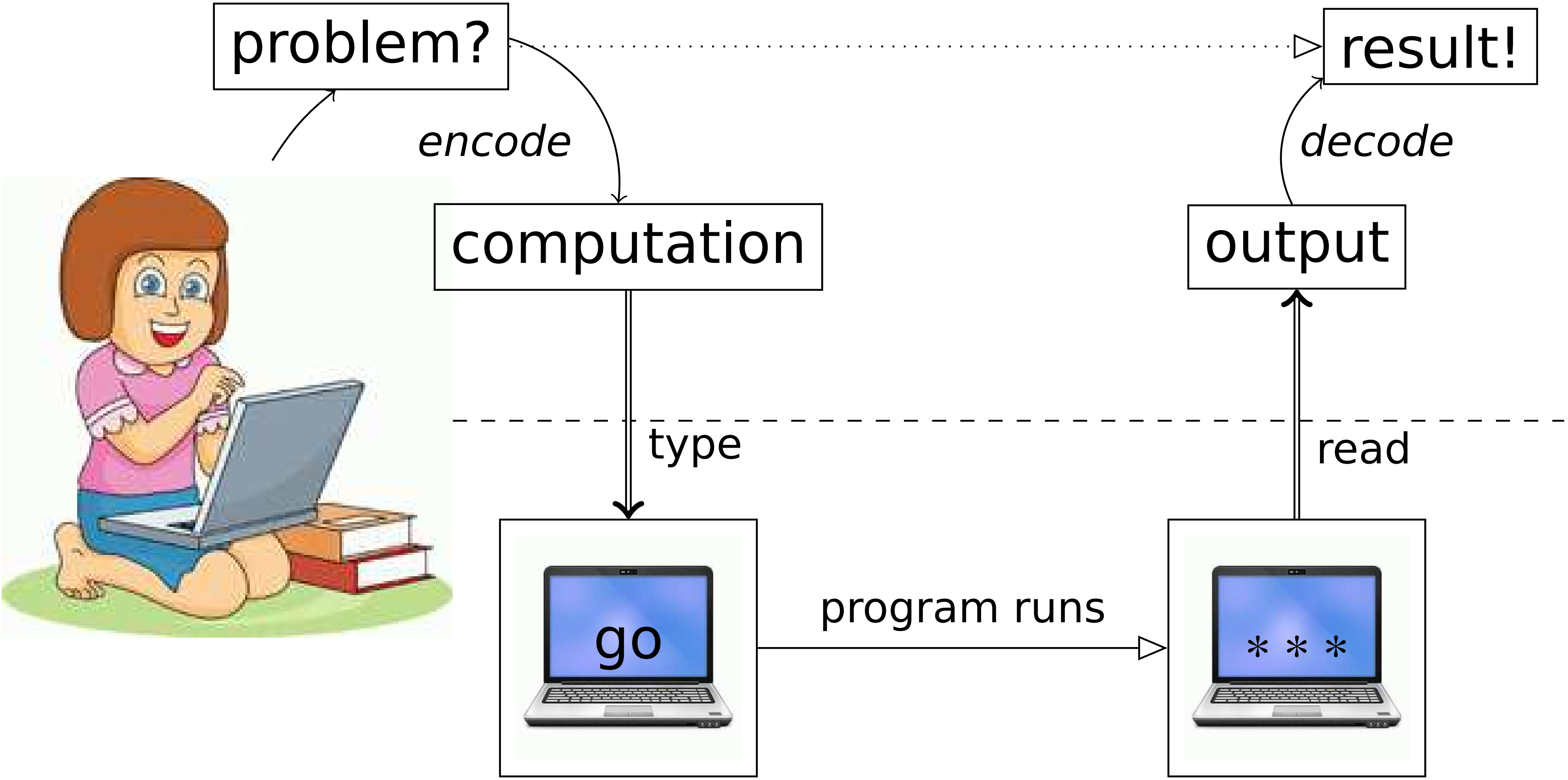
★ hybrid computational systems are the norm ★

**theory:** single paradigm:

- classical – Turing Machine
- analog – Shannon's GPAC
- quantum – gate model, QTM, CV, MBQC, QW, AQC, . . .
- linear optics (Bosons) [Aaronson/Arkhipov STOC 2011 ECCC TRI-10 170]

*many different quantum models: quantum circuit/gate model roughly corresponds to digital classical*

# computing




article: "When does a physical system compute? Proc. Roy. Soc. A 2014 **470**, 20140182

`http://dx.doi.org/10.1098/rspa.2014.0182` (Horsman/Stepney/Wagner/VK)

# quantum computing

input $\longrightarrow$ encode $\longrightarrow |\psi_{in}\rangle \longrightarrow \hat{U} \longrightarrow |\psi_{out}\rangle \longrightarrow$ decode $\longrightarrow$ result

$\hat{U}$ is unitary evolution (or more generally, open system/environment)
– can be gate sequence or engineer Hamiltonian $\hat{H}(t)$ such that

$$|\psi_{out}\rangle = \mathcal{T}\exp\{-i/\hbar \int dt\ \hat{H}(t)\}\,|\psi_{in}\rangle$$

★ covers most of quantum information processing . . .
. . . including communications, where aim is *result=input*

encode – arbitrary choices:

using spin-down $|\downarrow\rangle \equiv 0$ instead of spin-up $|\uparrow\rangle \equiv 0$ makes no difference
$\rightarrow$ provided encode and decode done consistently

# quantum information processing:

quantum computing (& quantum comms) built on the idea that:

**quantum logic** allows greater **EFFICIENCY** than **classical logic**

| **classical** | **quantum** |
|---|---|
| bits, 0 or 1 | qubits, $\alpha\|0\rangle + \beta\|1\rangle$ *coherence* |
| yes or no, binary decisions | yes and no, *superposition* |
| HEADS or TAILS, random numbers | random measurement outcomes |

⇒ quantum gives different computation from classical: *how different?*

- **computability** – what can be computed?
- **complexity** – how efficiently can it be computed?

★ quantum **computability** is the same as classical
**complexity** differs: some problems can be computed more **EFFICIENTLY**

# quantum advantage?

*how to translate quantum logic into better computing devices?*

depends on definition of **EFFICIENCY**

- *in theory:* *polynomial scaling with system size*
- *in practice:* *produces answers on human timescales*

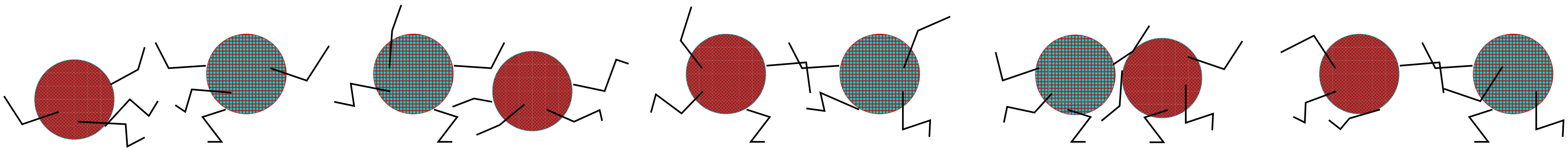
*roughly speaking:*

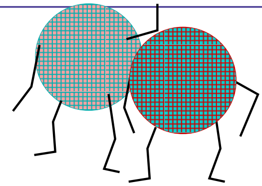
**quadratic** speed up exploits quantum coherence, interference effects

**exponential** speed up exploits parallelism in quantum superposition

★ comparison of real physical devices, not of mathematical theories

⇒ complexity theory alone won't tell you whether useful in practice





# quantum gates

**qubits**: 2-state quantum systems: *examples:* electron spin, photon polarisation
**localised**: distinguishable – no Fermi or Bose statistics to deal with

- choose a basis: $|0\rangle$ and $|1\rangle$ superpositions $\alpha\,|0\rangle + \beta\,|1\rangle$

input⟶ encode ⟶ $|\psi_{in}\rangle \longrightarrow \hat{U} \longrightarrow |\psi_{out}\rangle \longrightarrow$ decode ⟶result

$\Rightarrow$ how to apply $\hat{U}$ to the quantum state? $\hat{U}$ is “program” – could be any unitary
– efficient program needs efficient description

$n$ qubits: $\hat{U}$ is $2^n \times 2^n$ so efficient program = sparse matrix, $POLY(n)$ non-zero

decompose $\hat{U}$ into smaller operations applied to a few qubits at a time
★ important result: like classical, this is possible for quantum too ★

one entangling two-qubit gate + a few single qubit gates $\Rightarrow$ construct any $\hat{U}$

$\Rightarrow$ which universal gate set to choose?
– depends on physical system and error correction requirements...

# quantum superposition

consider three bits:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |

suppose we want to compute $F(x)$ for 8 different values of $x$ ?

run the program eight times, once for each value of $x$

$\Longrightarrow$ what if we could input all eight values at once?

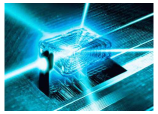
quantum mechanics lets us do this: **superposition:**

$$|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$$

no free lunch: get a superposition of all eight answers . . .

select one, find out which $x$ it corresponds to: quantum advantage!

how? $\uparrow$ smart quantum algorithms $\uparrow$



useful quantum computing needs **quantum algorithms**

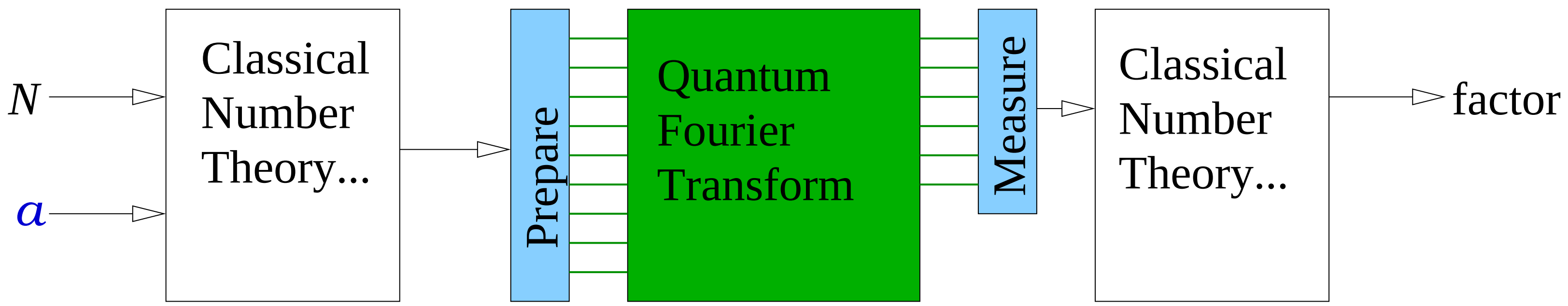
# factoring large numbers – is hard!

basis of crypto schemes, use numbers too large to factor classically

large enough **quantum computer** will break this: **Shor's algorithm**

**problem:** find a factor of a number $N = pq$

**algorithm:** first choose a co-prime number $a$




*classical* *quantum . . quantum* *classical*

★ the hard bit is to find $r$, the periodicity of $x^a$ (mod $N$) for $0 < x < N$

→ Fourier transforms good at this...QFT exponentially faster than FT
$a^{r/2} \pm 1$ gives a factor of $N$ (with high probability)

# how good is Shor's algorithm?

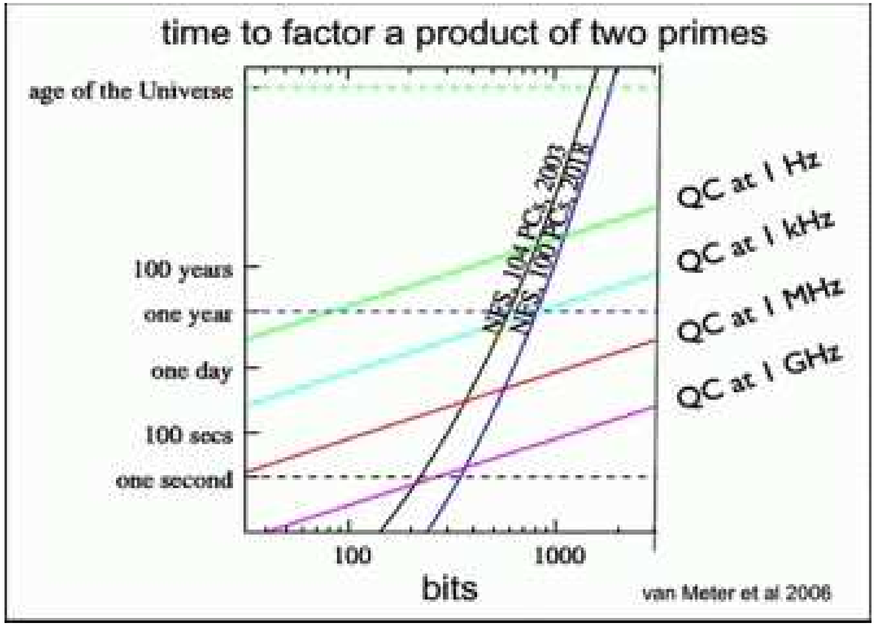
need to beat: best classical (2009): 232 digits (RSA-768) = 768 bits

Shor's algorithm for $n$-bits needs: $2n$ qubits in QFT register plus $5n$ qubits for modular exponentiation = $7n$ logical qubits $\rightarrow$ 768 bits need 5376 logical qubits

now add error correction: depends on error rates...
–if error rate close to threshold
– need more error correction

for low error rates, maybe 20–200 physical qubits per logical qubit; for high error rates, maybe $10^5$

suggests we may need Teraqubit quantum computers to break factoring – scaling favours quantum, but the crossover point is high
current h/w: factor 35 i.e., $n = 6$ bits




Quantum annealing (D-Wave) may challenge sooner: different algorithm – scaling $\sim n^2$ qubits; current h/w: 18 bit numbers [SciRep (2018) 8:17667]
$\rightarrow$ ~*1500 times larger RSA-768* – embedding o/h uncertainty for 147456 qubits

# encoding problems in qubit Hamiltonians

+ computational basis state $|j\rangle = |q_0 q_1 \dots q_k \dots q_{n-1}\rangle$ with $q_k \in \{0, 1\}$
+ superposition of all basis states:

$$|\psi_0\rangle = 2^{-n/2} \sum_{j=0}^{2^n-1} |j\rangle = 2^{-n/2} \left(|0\rangle + |1\rangle\right)^{\otimes n}$$

encode problem into $n$-qubit Hamiltonian $\hat{H}_p$

such that **solution** is lowest energy state (ground state)

example: find state $|m\rangle$ then $\hat{H}_p = \mathbb{1} - |m\rangle\langle m|$

$$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

example: three qubits, exactly one must be $|1\rangle$

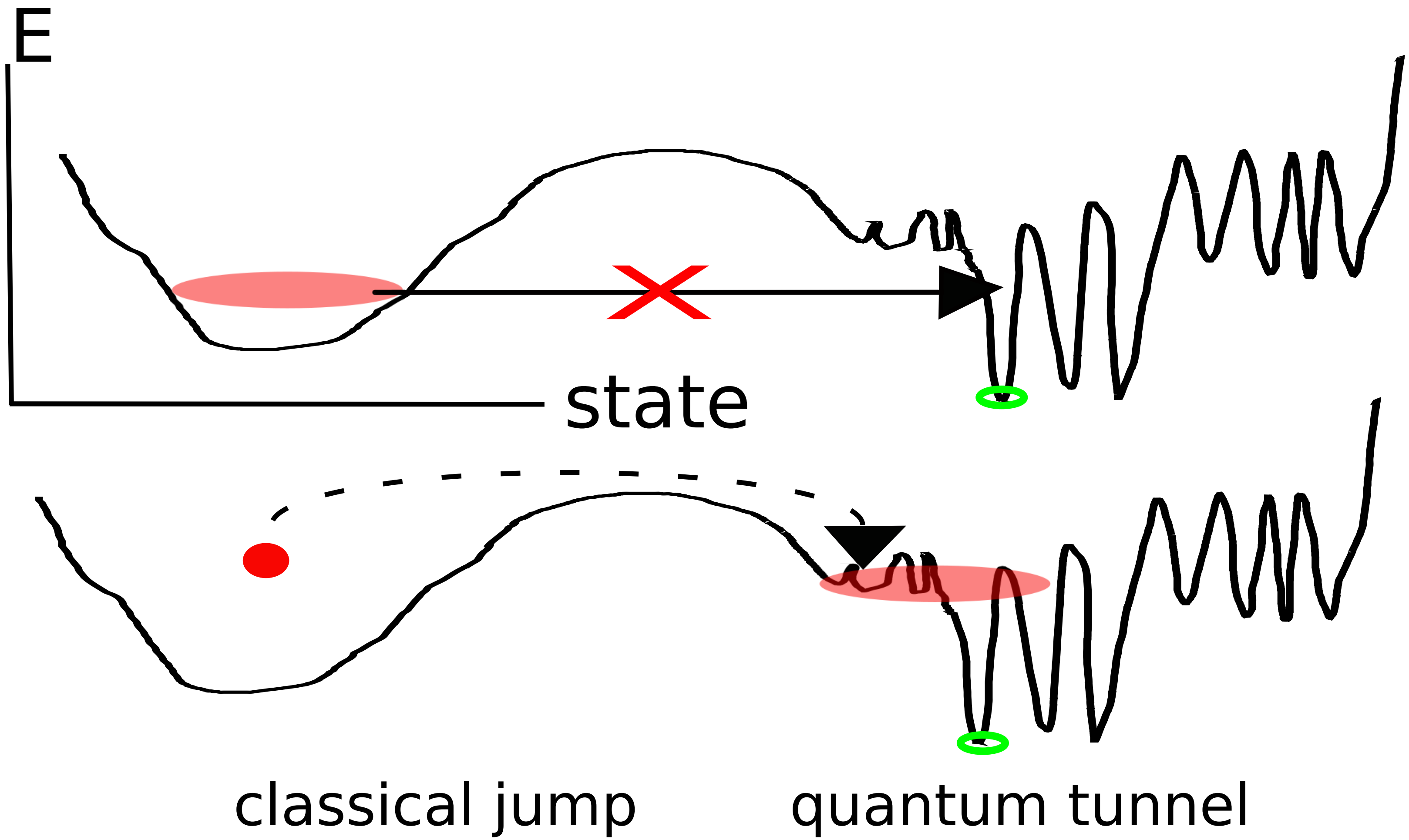
$$\hat{H}_p = (\mathbb{1} - \hat{Z}_1 - \hat{Z}_2 - \hat{Z}_3)^2$$

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Pauli-Z operator: $\hat{Z}\,|0\rangle = |0\rangle$ and $\hat{Z}\,|1\rangle = -\,|1\rangle$

# quantum annealing energy landscape

find the lowest point:




graphic credit: Dr Nick Chancellor, Durham University

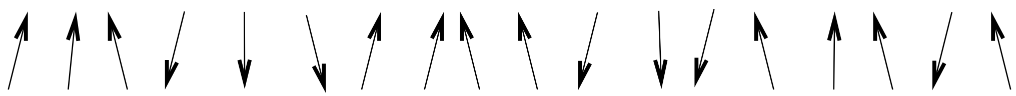
# beyond classical?

**simulating a quantum system:** example – $N \times$ 2-state particles
$\longrightarrow 2^N$ possible states – could be in superposition of all of them

**classical requires:**
one complex number per state: $2^{N+1}\times$size-of-double $\longrightarrow$ 1Terabyte holds $N = 36$
– each additional particle doubles memory required
compression methods can squeeze a little more [Chen et al arXiv:1802.06952, 64 qubits]
– *methods being developed for verification of early quantum computers*

100 qubits = well beyond exascale

if don't need to track all superpositions, larger classical simulations possible
(e.g., matrix product states, tensor networks . . .)



*classical is limited to subspace size $< 50$ qubits however large system is*

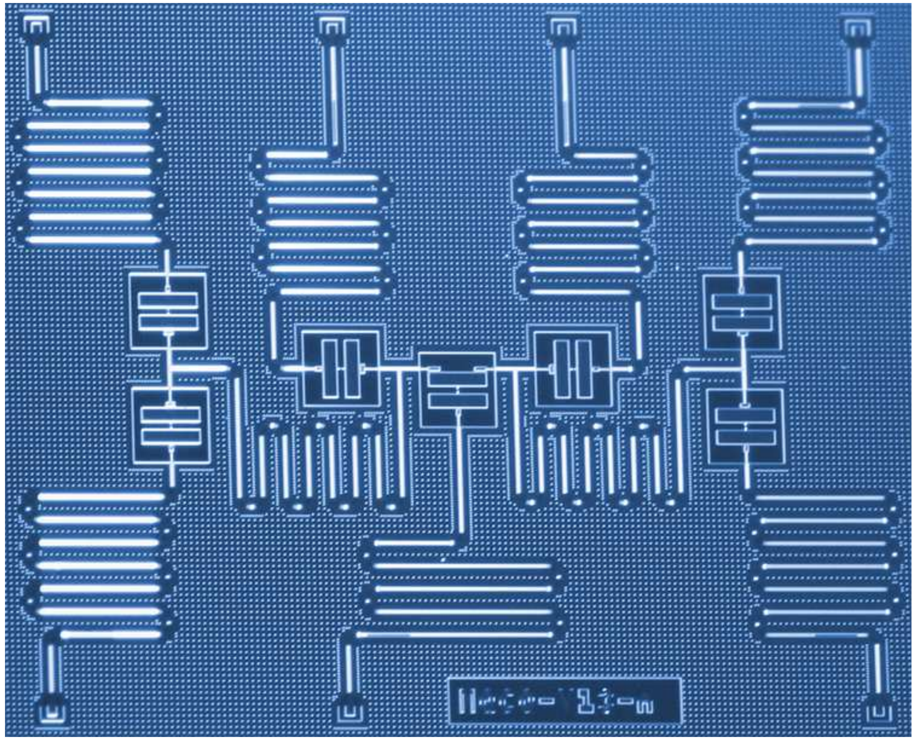
# who is building quantum computers?

→ universities and research centres are developing hardware and software . . .

also *many companies* – notably:

**have hardware they are talking about now:**

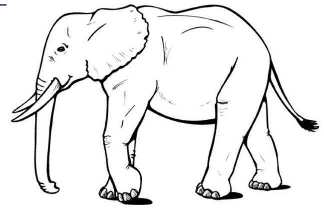
- IBM (Yorktown Heights, US)
- Google (Santa Barbara, US)
- D-Wave Inc, Vancouver, Canada)
- Rigetti (San Francisco, US)
  + *Rigetti UK with ISCF funding...*
- IonQ (Maryland, US) ions
- PsiQuantum (Palo Alto, US) photons



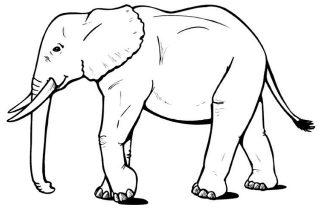
IBM 7 qubit chip

**how big?** IBM: 127 qubits like the above; D-Wave: 5,000 qubits *(noisy and not as powerful)*; ionQ: 32 low noise qubits, in 19" rack

# what I didn't cover:



*there are some elephants in the room ...*



- **quantum error correction** - not user level; resource intensive
- **quantum verification** - we know how (w/o exascale HPC)
- low level issues for integrating quantum computing with HPC
  = **timescales**, syncronisation
  = **data formats**, data type conversion

→ **we need**

- quantum computing experts
- HPC experts
- applications experts

**all working together**

⇒ ***to develop hybrid classical quantum algorithms for applications***

CCP-QC

# Collaborative Computational Project – Quantum Computing

*– facilitating quantum computing applications by networking between computational scientists and the quantum computing community –*

CCP-QC activities:

- joint meetings with other CCPs and the quantum computing community
- training days for computational scientists about quantum computing
- run small projects to develop proof-of-principle code and demonstrations on early quantum computing hardware – with STFC CoSeC support
- online information resource on scientific applications of quantum computing

`https://ccp-qc.ac.uk` @QC_CCP contact: info@ccp-qc.ac.uk

UKRI Engineering and Physical Sciences Research Council

UKRI Science and Technology Facilities Council

# Quantum Enhanced Verified Exascale Computing

★ **Strathclyde:** Viv Kendon (PI)
★ **Durham:** Richard Bower, Alastair Basden, Stewart Clark, Nicholas Chancellor, Halim Kusumaatmaja
★ **London Southbank:** John Buckeridge (KE)
★ **UCL:** Scott Woodley, Richard Catlow, Paul Warburton
★ **Warwick:** Animesh Datta

★ ExCALIBUR Cross-Cutting project:
*potential disruptor: quantum computing*

current – NISQ* era – quantum computers need near exascale classical to verify

⇒ challenge is to make this potential useful ⇐

[*NISQ = noisy intermediate-scale quantum]

★ *two use cases:* fluids sim and materials sim

systematic evaluation, identification, and development of relevant quantum algorithms for exascale subroutines

★ quantum VVUQ

★ methodology to apply to other use cases

★ *funders and partners:*

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME
Engineering and Physical Sciences Research Council
Quantum Computing & Simulation Hub
National Quantum Computing Centre
CCP-QC

**Q**uantum
**E**nhanced
**V**erified
**E**xascale
**C**omputing

★ *two use cases:* fluids sim and materials sim

systematic evaluation, identification, and development of relevant quantum algorithms for exascale subroutines

★ quantum VVUQ

★ methodology to apply to other use cases

# ★ opportunities and jobs

- *postdocs in:*
  - quantum verification (Warwick)
  - quantum computing (Strathclyde – live!)
  - fluids simulations (Durham – soon ...)
  - materials simulations (UCL – soon ...)
- *PhDs in:*
  - Reliable quantum simulations of plasma and fusion physics (Warwick)
  - Hybrid quantum algorithms (Strathclyde)
  - UCL CDT ...

★ *funders and partners:*

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME
UKRI Engineering and Physical Sciences Research Council
Quantum Computing & Simulation Hub
UKRI National Quantum Computing Centre
CCP-QC