Quantum computing

Introduction and why we should care about it

Matthew Viljoen

EGI Foundation, Service Delivery and Information Security lead

21 October 2026

EGI Quantum Computing webinar

TLP: WHITE Public

Outline

- Quantum computing vs classical computing
- Bits and qubits and different QCs
- Applications and use-cases
- Status at present
- Takeaways and relevance for EGI

Quantum vs classical computing - bits and qubits

Classical 'bit' – either 1 or 0 (never both)
e.g. voltage on a wire -> encoding data in binary;
Deterministic -> we always know what state we have



Quantum bit 'qubit' – the Quantum Mechanical (QM) generalization of a bit. Also can store information … but in a very different way!

Qubit = a weighted blend of 0 and 1 at the same time! Called a 'superposition'
e.g. spin up/down of an electron; paths of a photon

How can qubits help us in computing?
We can use QM phenomena like superposition, interference and entanglement to tackle a class of problems exponentially faster than with classical computing

A little bit more about qubits (II)

Superposition: until you *measure* a qubit it exists in a combination of two possible states: |0› and |1›

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers whose squared magnitudes add to 1 *i.e.* $|\alpha|^2+|\beta|^2=1$

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

State vectors of a single qubit in 2-d complex vector space

Entanglement: ≥2 qubits 'linked' and share an intertwined quantum state, creating correlations between their measurement outcomes. These quantum relationships can be harnessed as a computational resource.

Scaling considerations

Bits: *n* bits = stores one of 2^n possible combinations at a time

Qubits: *n* qubits stores **ALL** of 2^n possible combinations at a time!

No. of qubits	Classical storage required to list states (complex amplitudes)
30	1GB
40	1TB
50	1EB
100	≈2.0×10^{13} EB
300	≈3.26×10^{91} bytes – more atoms than in the universe! (~10^{80})

Bits and qubits (III) and different QCs

Measurement differences:

Bits: 1 or 0 as you would expect, *deterministically*

Qubits: Measurement results in a collapse of the superposition to 1 or 0 probabilistically.

Multiple runs are needed to collect statistics encoded in these probabilities.

OK…But what actually *is* a qubit?

A pair of quantum systems (|0> and |1>) whose state can be manipulated

e.g:

- Superconducting qubits (used by Google, IBM)
  tiny microwave circuits at ~10 mK
- Trapped-ion qubits (IonQ, Honeywell/Quantinuum)
  individual charged atoms held in an electromagnetic trap
- Photonic qubits (PsiQuantum, Xanadu)
  photons within optical systems
- Spin qubits or silicon quantum dots (Intel, Diraq)
  electrons confined in semiconductor nanostructures
- Neutral atoms of Rb, Cs, Sr, Yb (Pasqal, QuEra)
  held in optical tweezers



Use cases

Use-Case reality check		
Task	**Quantum advantage?**	**Why?**
Web browsing, spreadsheets, video	No	No quantum advantage; overhead not worth it.
Ordinary integer addition	No	Classical adder circuits compact and deterministic
Factoring large integers	Yes	Superposition+interference discovers factors exponentially faster (Shor's algorithm)
Quantum simulation of molecules and materials	Potential: major focus for research	Quantum hardware can directly represent/evolve quantum states
Unstructured searches	Potential theoretical quadratic increase of speed	Grover's algorithm requires $O(\sqrt{N})$ DB queries rather than $O(N)$.
Monte Carlo simulation	Potential theoretical quadratic increase of speed	Quantum amplitude estimation potentially improves sampling complexity from $O(1/\varepsilon 2)$ to $O(1/\varepsilon)$

Status at present

From noisy processors towards fault-tolerant quantum computing

We're now in the 'Noisy Intermediate Scale Quantum Era'

- **Current QC technology is all noisy and error prone**
  - **Frequently break down, lots of maintenance**
  - ***Workaround: using multiple qubits to represent a single qubit***
- **Quite slow ~100 circuits per second**
- **QCs: Not physically fast but already useful for some applications**

Oct 22, 2025: Google Quantum AI announces first verifiable quantum advantage

Out-of-time correlator (OTOC) algorithm executes about 13,000 x faster on 65 qubit Willow SC compared to classical supercomputer

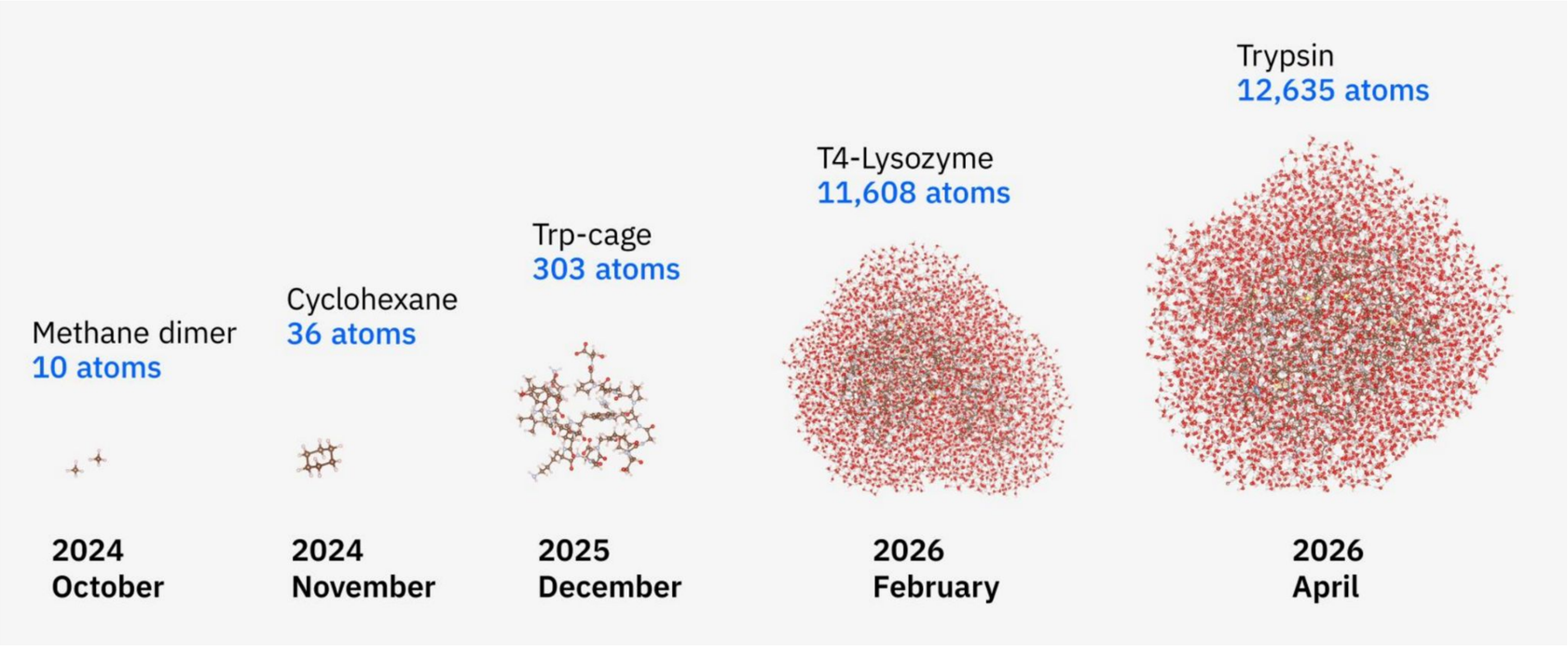
Real science research already being done thanks to QC

e.g.

- **Accelerated drug development (IonQ + AstraZeneca + AWS + NVIDIA)**
  - **Hybrid workflow for Suzuki–Miyaura reaction**
  - **20× speed-up over pre quantum-classical methods.**
- **Solutions of classes of multiple variable optimization problems**

Example application: Quantum-assisted protein chemistry

IBM: Quantum-contric supercomputing simulates a 12,635-atom protein (blog)



- **Quantum + supercomputer simulation of protein complexes**
- **Concrete example of help with real scientific computing workflows**

PKI and threats to cryptography

- Shor’s algorithm poses real threat to widely used PKI approaches
- Reality: today’s QCs can’t yet break RSA-2048
- New post-quantum cryptography standards now exist. Migration planning happening now.

Takeaways and relevance for EGI

- National labs starting to procure QCs
- QCs - not yet commodity (by a long shot!)
- Standards surrounding QC are in their early stages

But

- QC impact likely to become large
- AI + QC = could have a potentially huge impact
- EGI needs to follow QC landscape and incorporate QC into its future strategy

Global research engagement for QC

- RDA event in 2025: global expert discussion roundtable (inc. EGI)

  RDA and Microsoft White Paper: From HPC to Quantum - Shaping the Future of Research Computing

  Outcomes:
  - Setup hybrid HPC/AI/quantum infrastructure
  - Ensure democratised access while addressing global internet connectivity gap
  - Accelerate the adoption of post-quantum cryptography standards
  - Bridge the talent gap by integrating quantum/HPC fundamentals & ethics into STEM curricula

Maybe setup an Interest Group via RDA for following QC?

Thank you

Contact us

matthew.viljoen@egi.eu

Let's talk. Or meet in person.

Get in touch with us

www.egi.eu

This work is partially funded by the EU research and innovation programme