The Institution of Engineering and Technology

Quantum: Game-changer or niche?

16 May 2024

Welcome

The hybrid event will start at **7:00pm** at the Atrium, University of Suffolk and via Microsoft Teams.

Introduction: Kevin Foster FIET, Chairman, IET Anglian Coastal Local Network.

Presenter: Andrew Lord, Senior Manager of Optical Research, FIEEE & BT Fellow

Questions: Please type in your questions to the Q&A feature in Teams or be ready to ask them in the Atrium and these will be taken at the end of the presentation.

Close: Approximately 8:15pm

BT Group

Quantum – Game Changer or Niche?

Presenter:
Andrew Lord

Thursday 16th May 2024

Acknowledgements (too many to list but here are some key people) – Cathy White, Paul Wright, Zoe Davidson, Emilio Hugues-Salas, Dan Gilks and team. Also BT leadership including Tim Whitley, Paul Crane, Ian Hawkins, Maria Cuevas, Gabriela Styf Sjoman, Steve Taylor for their vision
AND MANY MORE

Flow

1. Quantum – what do we mean by it? What is it good for?

2. The quantum communications story from security to the quantum internet

3.What's happening in the UK and around the world?

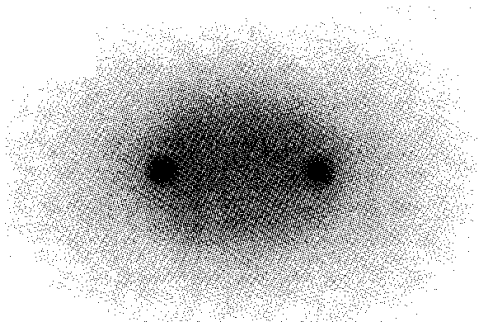
4. Some recent projects

5. Conclusions

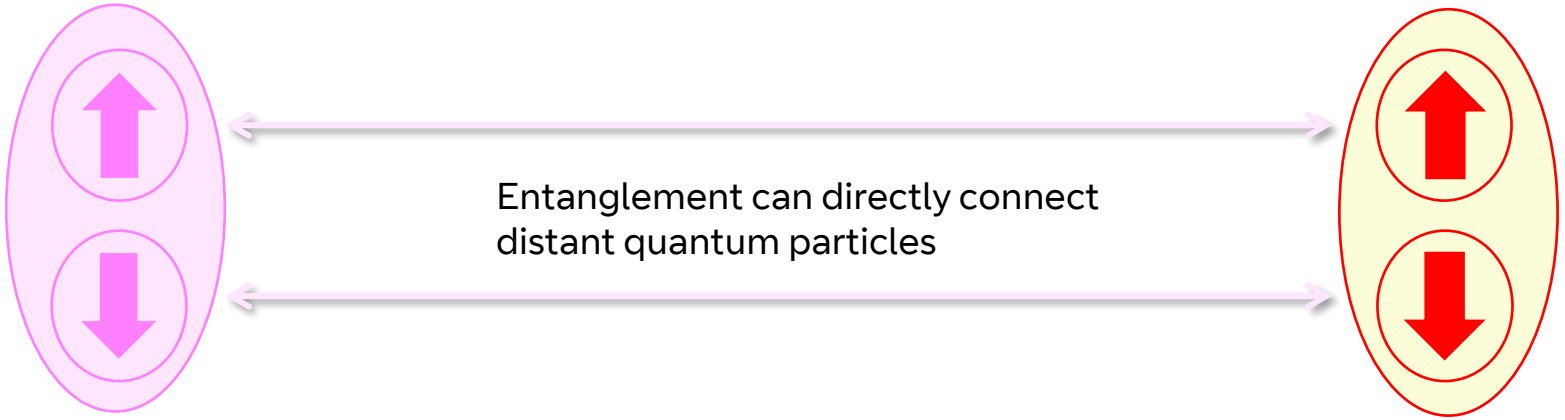
6. Game-changer or niche?

What do we mean by quantum?

Large, macroscopic objects have precise location, energy, velocity



Small, microscopic particles (atoms, photons, electrons) have innately uncertain locations, energies, velocities, spins, phases…



Entanglement can directly connect distant quantum particles

Small things can be in multiple states at once AND can affect each other INSTANTLY even though they are separate

And what can it do?

- **QUANTUM BITS – QUBITS**
  Multiple simultaneous states can be harnessed – encoding information onto atoms, photons in the form of QuBits
- **QUANTUM COMPUTERS**
  QuBits can be entangled together to dramatically increase computing power compared to classical computers
- **QUANTUM SECURE COMMS**
  Qubits can't be observed without changing them – leading to ultimate security
- **SENSORS**
  They are also extremely sensitive, make the most accurate clocks, brain scanners etc

Two VERY strange things about quantum states:

1. **If you measure, observe, look at, interfere with a single photon in-flight – you will change its state irreversibly. You cannot help it and you can't 'put it back'**

   This basic quantum mechanical principle allows us to set up innately impossible-to-tap communications

   Both good and bad guys can use this to send unhackable communications over optical fibre and free space links

   e.g. It wouldn't be possible for government agencies to tap communications should they need to

2. **Multiple photons can be entangled – such that observing one INSTANTLY affects the others, WHEREVER they happen to be in the universe at that moment!!**
   A quantum computer program consists of the specific entangled configuration of an ensemble of particles – which are then left to 'relax' from this initial state (the problem) into a final state (the solution)

Because (i) a quantum computer of Q qubits can represent 2^Q states (such that 100 qubits is already vastly bigger than a classical computer's capacity) and (ii) entanglement changes can instantly impact all qubits, a quantum computer can potentially quickly solve problems that would take classical computers billions of years

Introduction to the maths

$|\ >$ A quantum state expressed in bra-ket notation, introduced by Paul Dirac

Here I refer to spin, but it could also be position, phase etc

$\Psi = |\uparrow>$ Wave function for a particle definitely spinning up

$\Psi = |\downarrow>$ Wave function for a particle definitely spinning down

$\Psi = (1/\text{sqrt}(2)\ \{\ |\uparrow> + |\downarrow>\}$ This represents a single particle wave function with equal probability of spinning up and down. As its spin is observed, it will pick one of these states

1st particle *2nd particle*

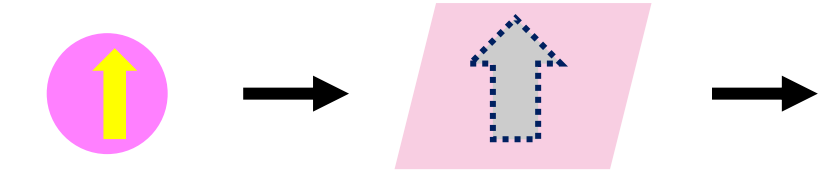
$\Psi = |\uparrow\downarrow>$ Wave function for two particles. First one is definitely spin up, whilst the second definitely spin down

$\Psi = (1/2)\ \{\ |\uparrow\uparrow> + |\uparrow\downarrow> + |\uparrow\downarrow> + |\downarrow\downarrow>\ \}$ Wave function for two independent particles – the state of one doesn't affect the state of the other

$\Psi = (1/2)\ \{\ |\uparrow\uparrow> + |\downarrow\downarrow>\ \}$ Two particle entangled state. Either particle can be either up or down. But as soon as one particle is observed, the other one will immediately adopt the same state as the measured particle.

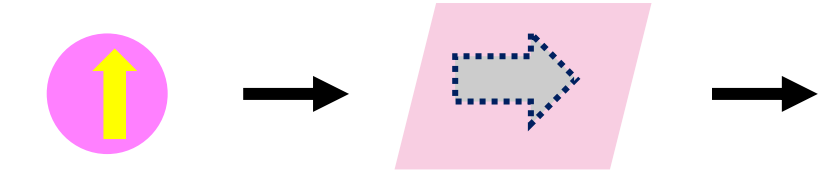
If you can create states like this, then you have made something very strange!

Quiz time!!!



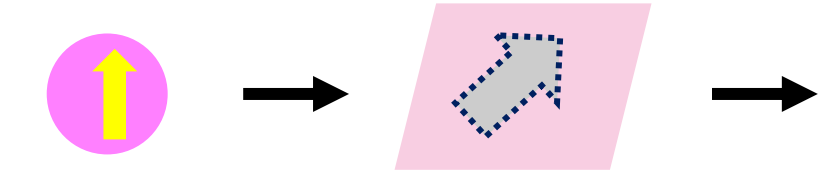
Light polarised vertically

Polariser sheet aligned vertically



Light polarised vertically

Polariser sheet aligned horizontally



Light polarised vertically

Polariser sheet aligned at 45 degrees

a. High intensity light
b. Single photon at a time

Quantum Technology Areas

Quantum Technology	Overview	BT involvement in this space
Quantum Computing & Simulation	Solving problems too complex for classical computers	• Experience with quantum computer languages • Hard problem classification • Quantum hackathons
Quantum Secure Communications	Preventing hackers from intercepting transmission by encoding it on single photons of light	• Running a commercial quantum trial in London • Leading on assurance • Researching next gen entanglement-based security
Quantum Sensing & Measurement	Atoms and photons are incredibly sensitive, enabling highly sensitive sensors	• World-leading RTydberg quantum radio receiver • Trialled quantum gravity sensors
Quantum Clocks & Timing	Orders of magnitude more accurate than conventional clocks	• Quantum clock technology • Accurate timing distribution • Overall network timing simulations
Quantum Imaging	Ultra sensitive imaging for (e.g.) military applications	• Limited activity

BT's 30-year quantum journey

Early R&D in the 1990s with patents around QKD for PON

Re-ignition of interest in 2013 due to:
- Quantum computer progress with risk to cryptography
- Maturing of QKD technology

We have built a range of demonstrators and trials
- Integrated QKD + classical WDM with Toshiba and Adva
- Customer QKD trial with ***National Composite Centre*** in Bristol – with
Toshiba and Adva – over Openreach commercial fibre product

London Quantum Secured Metro Network – launched April 2022

Other activities include:
quantum computers, quantum timing , sensors, QKD assurance, standardisation, satellite

1994	Early patents on QKD over PON
2013	BT + Toshiba first discussions on QKD + network integration
2018	BT Cambridge QKD link
2020	BT + Toshiba first customer trial with NCC in Bristol
2022	**Launch of London QKD metro trial**
2023	HSBC announced as major new triallist

An aside on cryptography – it's all about secret keys…

To send data securely from A to B

- Data needs to be encrypted at A
- And decrypted at B using the SAME key

Symmetric encryption.
Thought to be very strong.
Commonly uses AES256 protocol

To get this key from A to B can be done in various ways

- Suitcases and padlocks
- Other secrets

Key Distribution prior to data encryption

But the MAIN method uses another key – or a pair of keys

- Public Key Cryptography (e.g. Diffie-Hellman, RSA)
- A uses B's public key to encrypt the symmetric key
- B uses his private key to decrypt it

Public Key Crypto (PKC) uses a pair of keys to transfer a single secret key

Quantum computers put PKC at risk

Shor's algorithm could break some PKC algos in the future

New methods of distributing keys are being actively developed:

- Quantum Key Distribution (QKD)
- Post Quantum Cryptography (PQC)

A Quantum Computer, using Shor's Algorithm, could break much of the world's security in a few years

Shor's algorithm attacks Public Key Cryptography

The relationship between public and private keys depends on the ability to factorise an enormous number
Quantum computers can employ a short-cut to performing this factorisation without having to search all possibilities

But when?

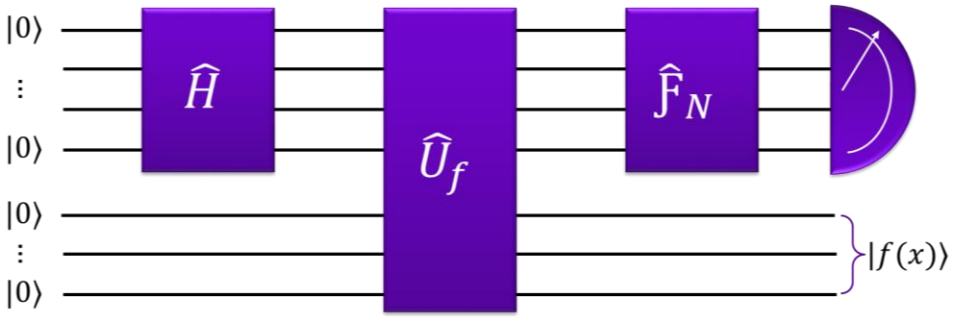
RSA generally uses a 1024-bit key
Therefore a quantum computer with at least 1024 qubits would be needed
In fact we will need many more qubits than this due to imperfect quantum gate operations

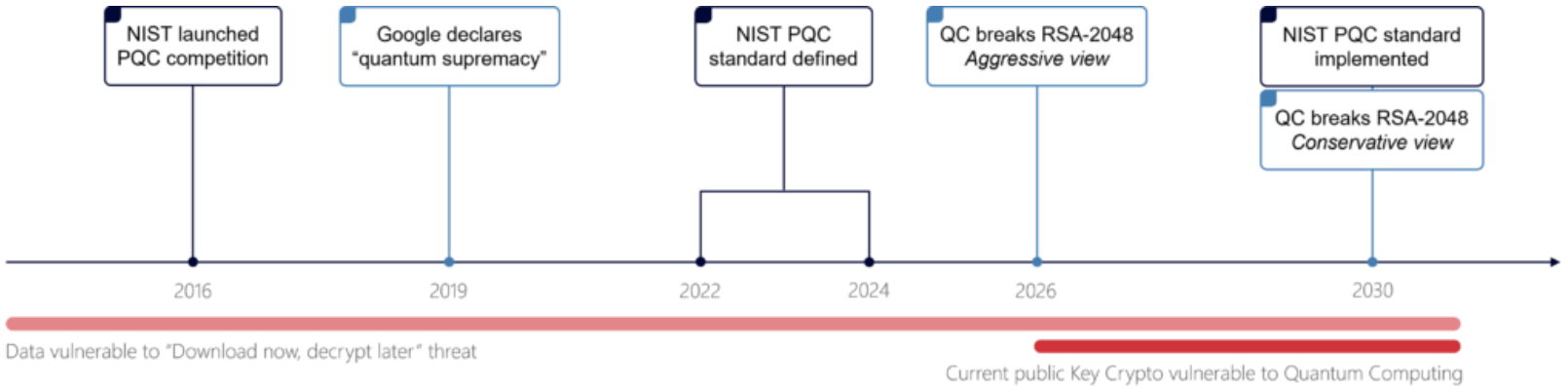
Crucial to develop alternative key distribution approaches

Post Quantum Cryptography

New algorithms hopefully less susceptible to QCs
Could take many years to fully implement these

Shor's quantum computer algorithm for breaking PKC





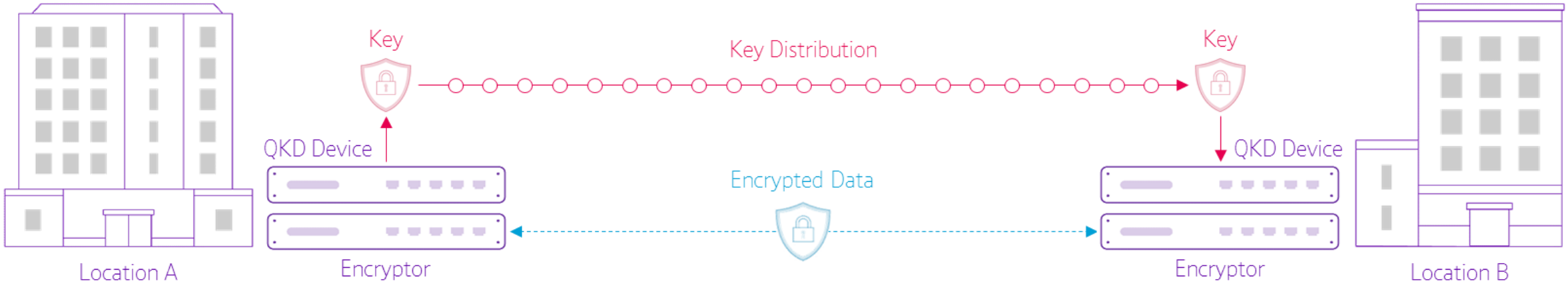
What is Quantum Key Distribution?

QKD distributes encryption keys by encoding information on streams of photons of light that is impossible to hack during transmission and provides guaranteed secrecy

Encryption keys are formed out of a stream of single photons

Photons carry keys using phase, polarization, or position modulation

The key is refreshed constantly



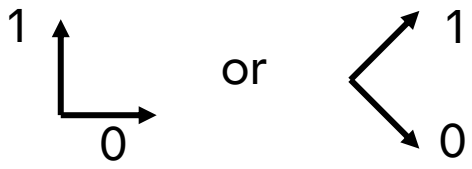
QKD is secure for two reasons: (i) if a hacker steals a photon, it doesn't get through and hence can't be used to form a key, (ii) any attempt to clone, copy or even simply OBSERVE the photon goes immediately detected.

In Quantum Physics, all observations irreversibly change the system being observed – if you look at it, you change it!

QKD basis states

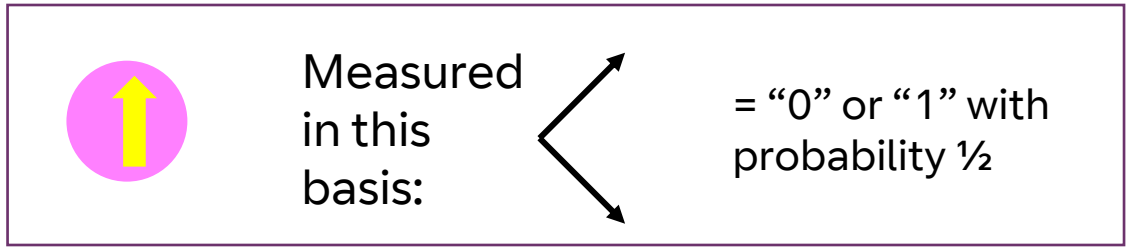
Photons carrying keys are sent by Alice as a stream of 0s and 1s

Each key randomly uses one of two basis states:



If Bob measures the photon using the SAME basis state
He will get the correct result

If Bob guesses wrong, he will get a random result



In QKD, both Alice and Bob randomise their choice of basis states for each photon

They then compare which basis states were used. They keep all results where they used the same basis states

Hackers can be detected by randomly comparing a small % of bits and looking for inconsistencies

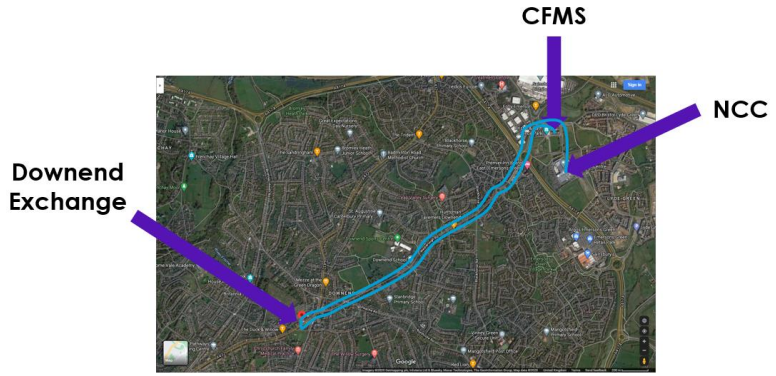
NCC* QKD solution - 2019

ISCF Innovate UK funded project

How to design a QKD-secured data link between two NCC buildings

Using all commercially available products, including the fibre access

- Toshiba QKD solution – carefully designed for working alongside classical channels
- Adva ethernet transmission solution – 10GE with external key input feature
- Openreach OSA filter connect fibre product – provides managed access to 8 / 16 channels optical spectrum



NCC – National Composite Centre in Bristol

London Quantum Secured Metro Networks Trial

Connecting sites in London's Docklands, the City and the M4 Corridor

- The new network is the world's first commercially viable trial of a quantum network infrastructure that transmits keys and data over a common bearer .
- It provides a range of quantum-secured services including dedicated high bandwidth end-to-end encrypted links.
- The QKD links are provided using a quantum network that includes both core and access components and is fully integrated into BT's existing network management operations.

- Toshiba provide quantum key distribution hardware and key management software.
- The initial trial service encompasses BT-generated keys, encryption and transmission on the key bearing transmission.
- Subsequent trial services will encompass BT-generated keys, encryption, and transmission on other non-key bearing Optical , Ethernet or IPvpn circuits.

BT's London Quantum-Secured Metro Network

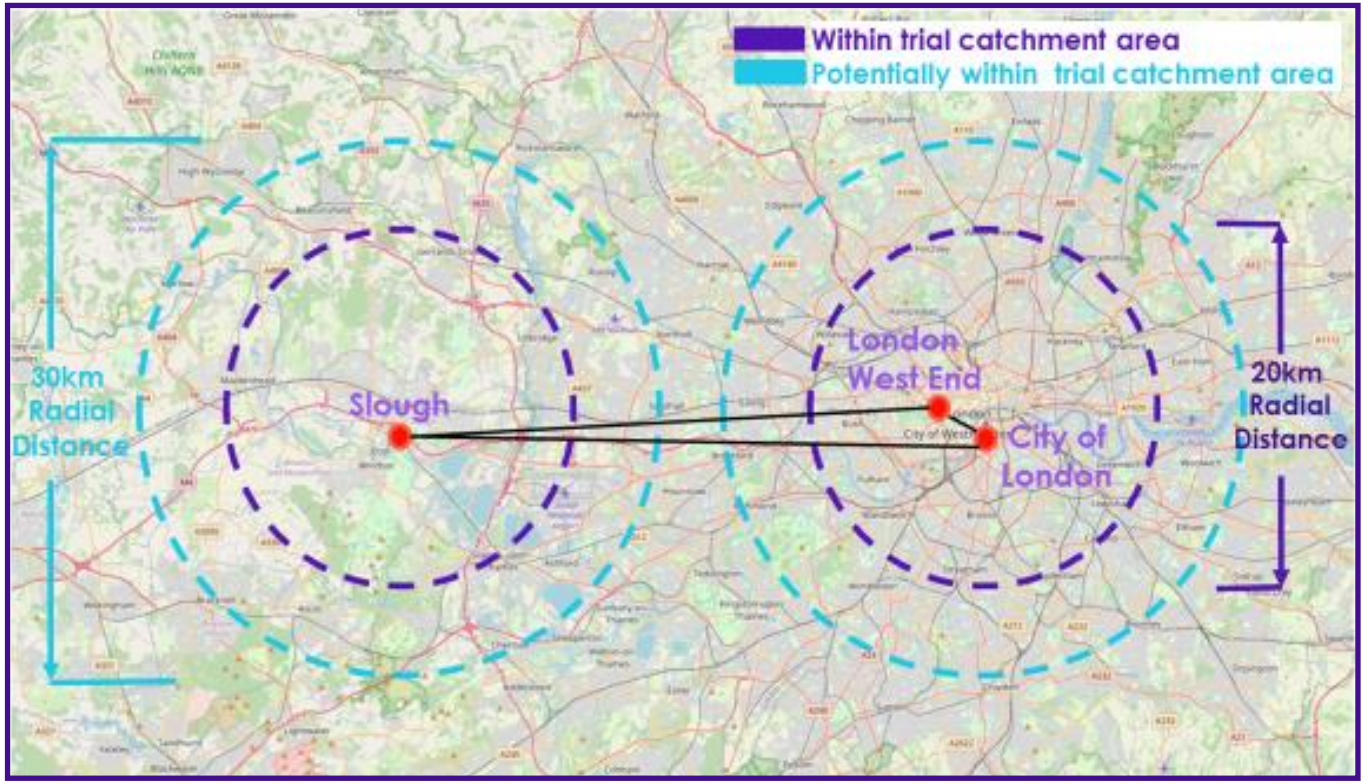
Launched April '22
Currently supporting EY and HSBC
With partners Toshiba, AWS, Equinix

What:

- 3-year metro-based QKD trial with Toshiba
- 3 node ring
- Connections to trial customer sites
- SDN-based network + security management
- Scope for satellite QKD ground station
- Multiple Networks teams

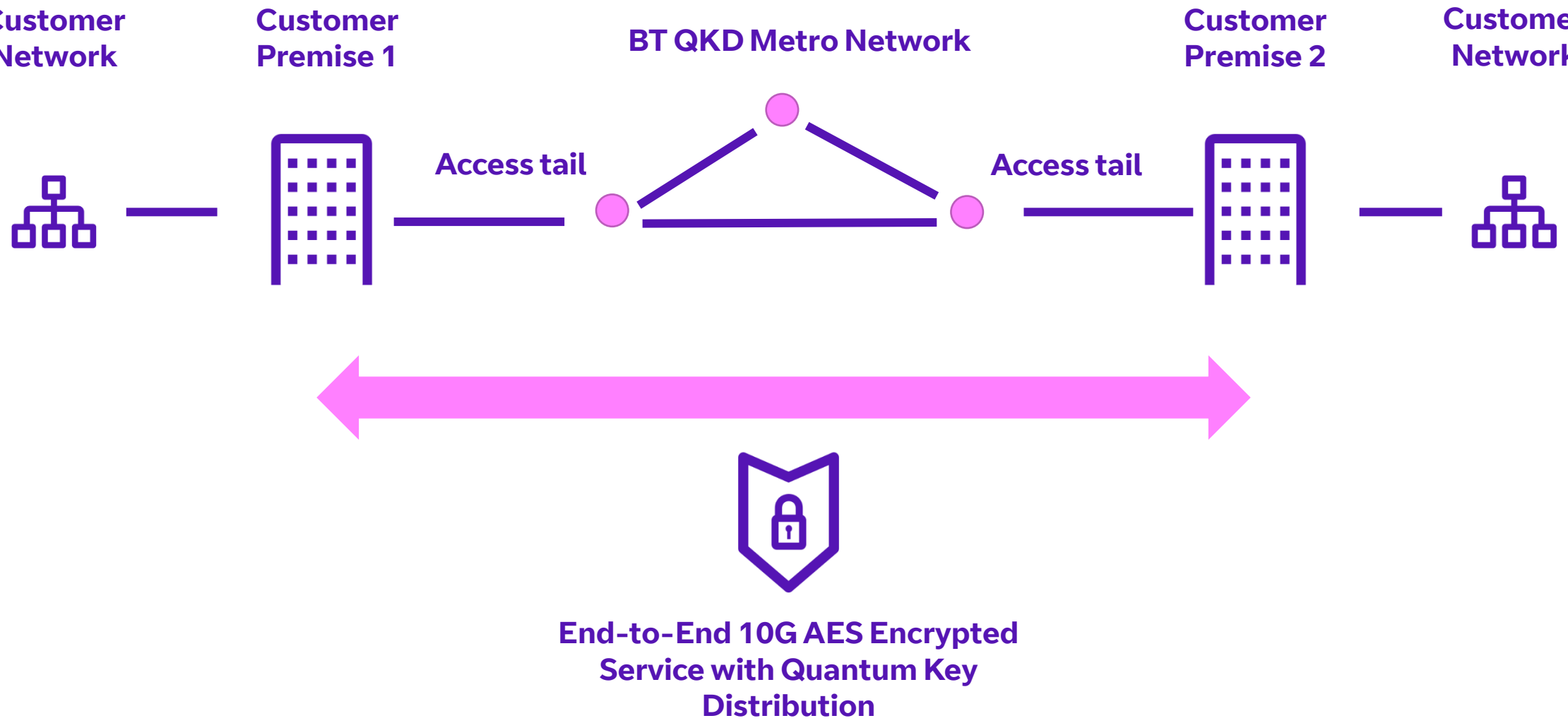
Why:

- Ambition for UK QKD commercial service
- Design and testing of equipment / networks
- Validation of markets and use cases



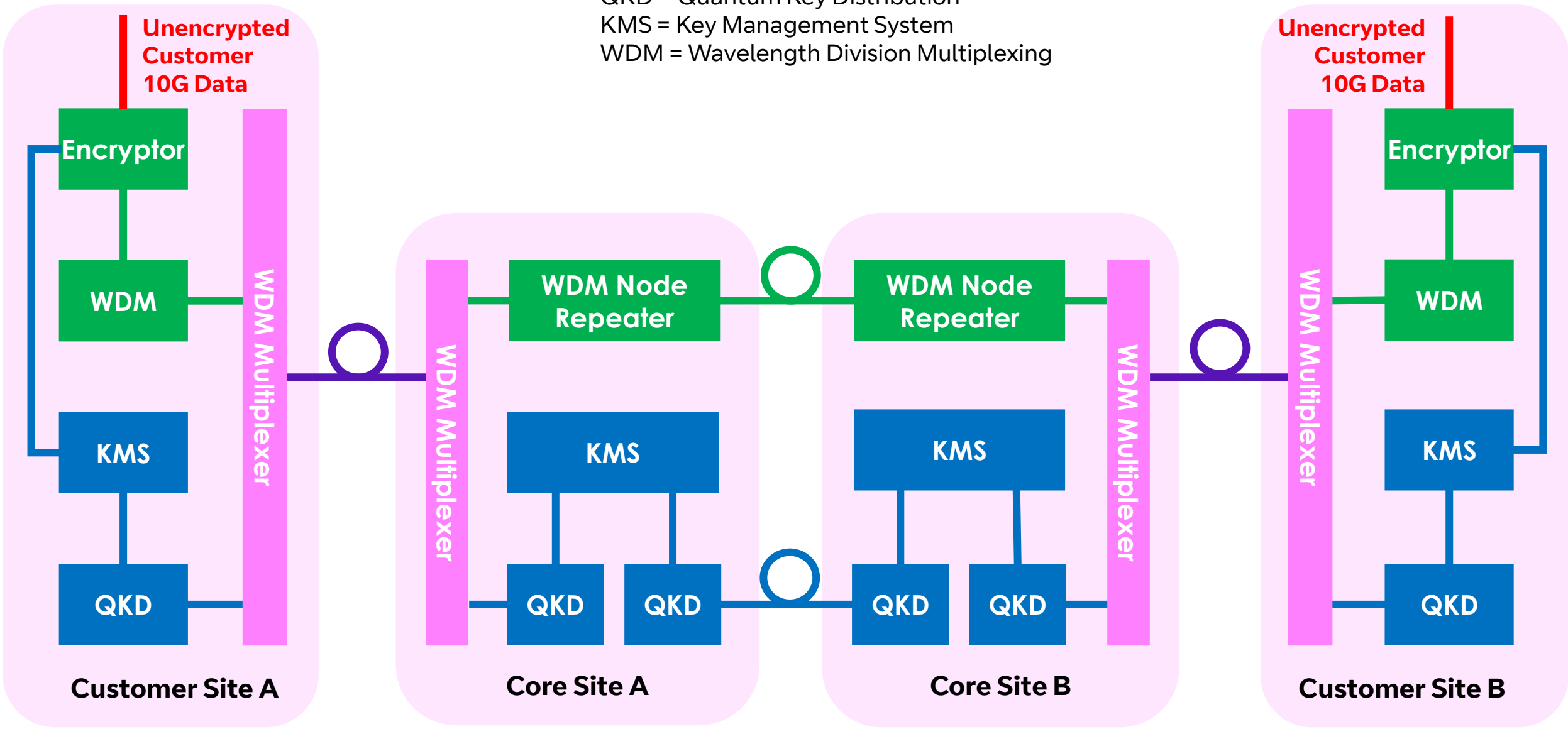
Plan to continue this trial until at least April 2025 (3 years), on-boarding additional customers

QSMN Overview Diagram

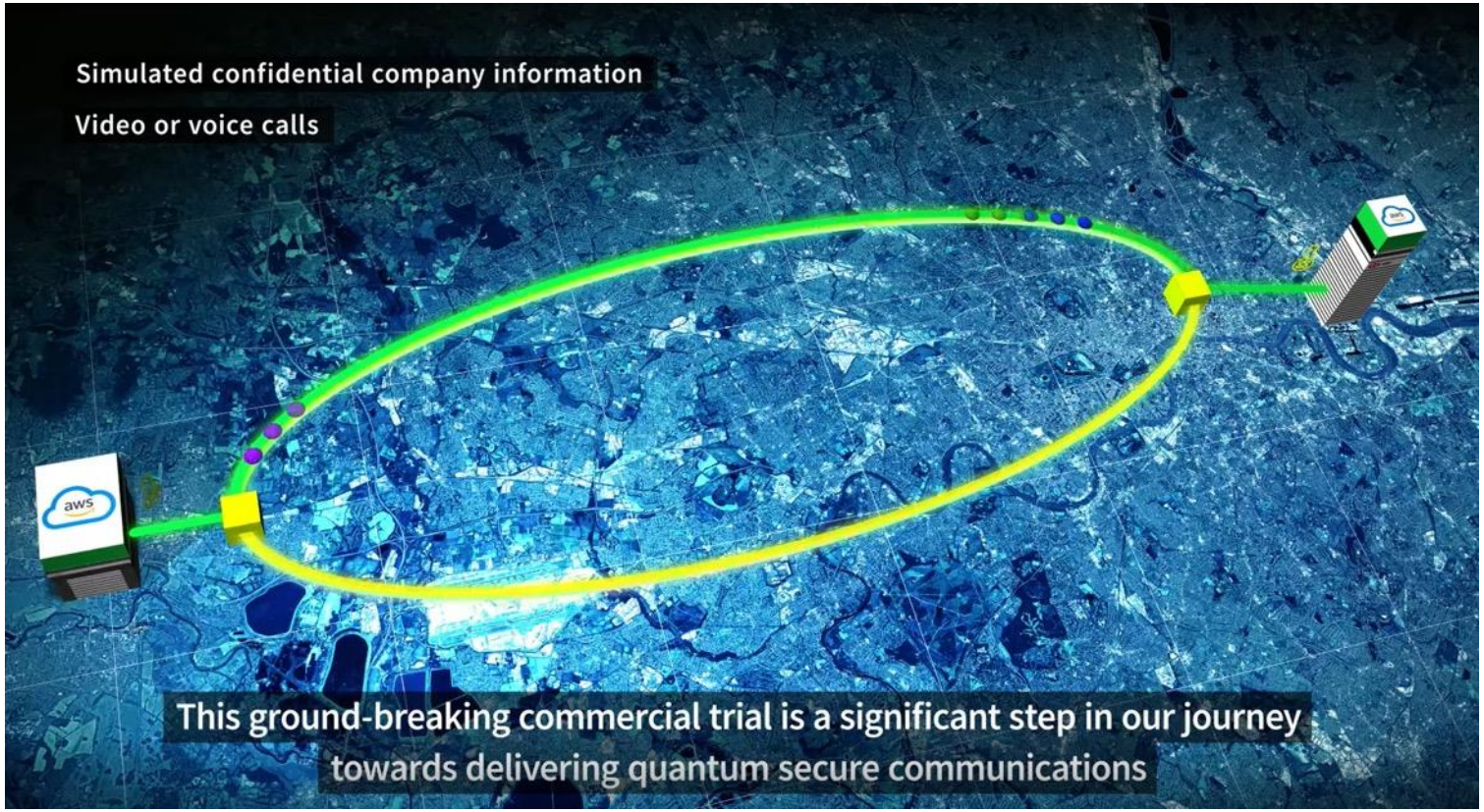


Design Details

QKD = Quantum Key Distribution
KMS = Key Management System
WDM = Wavelength Division Multiplexing



BT/Toshiba Quantum Metro Network – Initial Use Cases



SLIDE TAKEN FROM HSBC PRESENTATION

Cloud-to-cloud interconnectivity

Videocall

Financial transactions

Combining QKD with PQC

Quantum communications Roadmap

Quantum Key Distribution (QKD) under commercialisation now

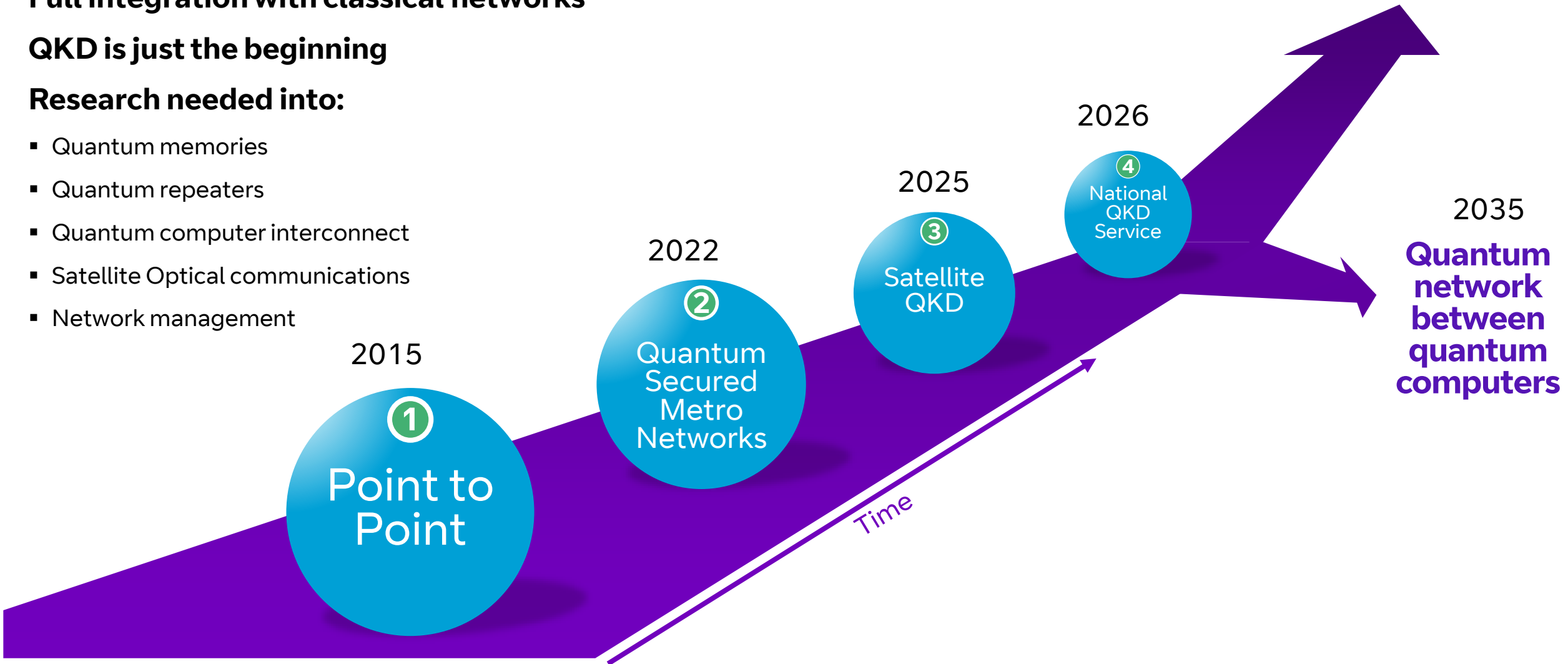
National quantum networks will evolve for the next 15+ years

Full integration with classical networks

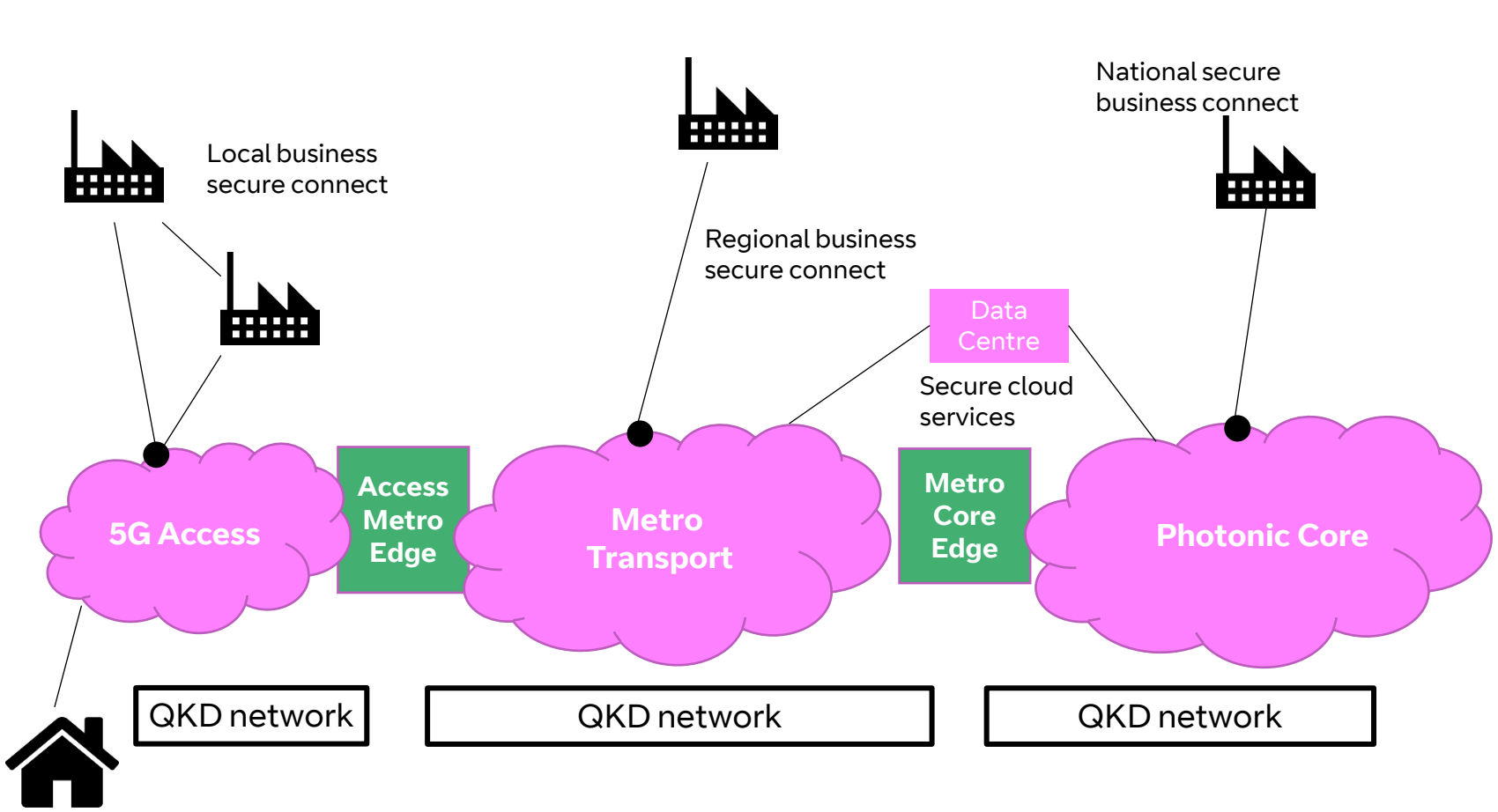
QKD is just the beginning

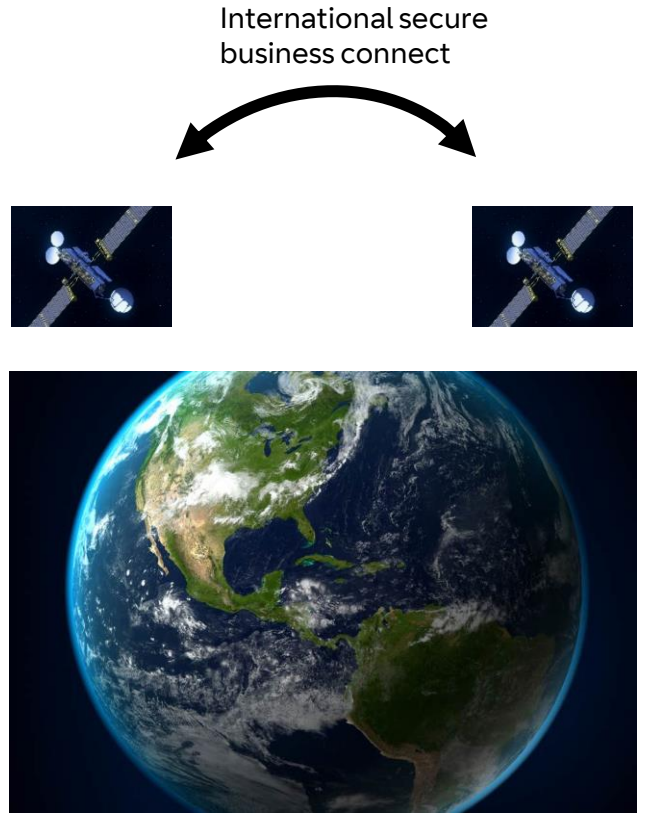
Research needed into:

- Quantum memories
- Quantum repeaters
- Quantum computer interconnect
- Satellite Optical communications
- Network management



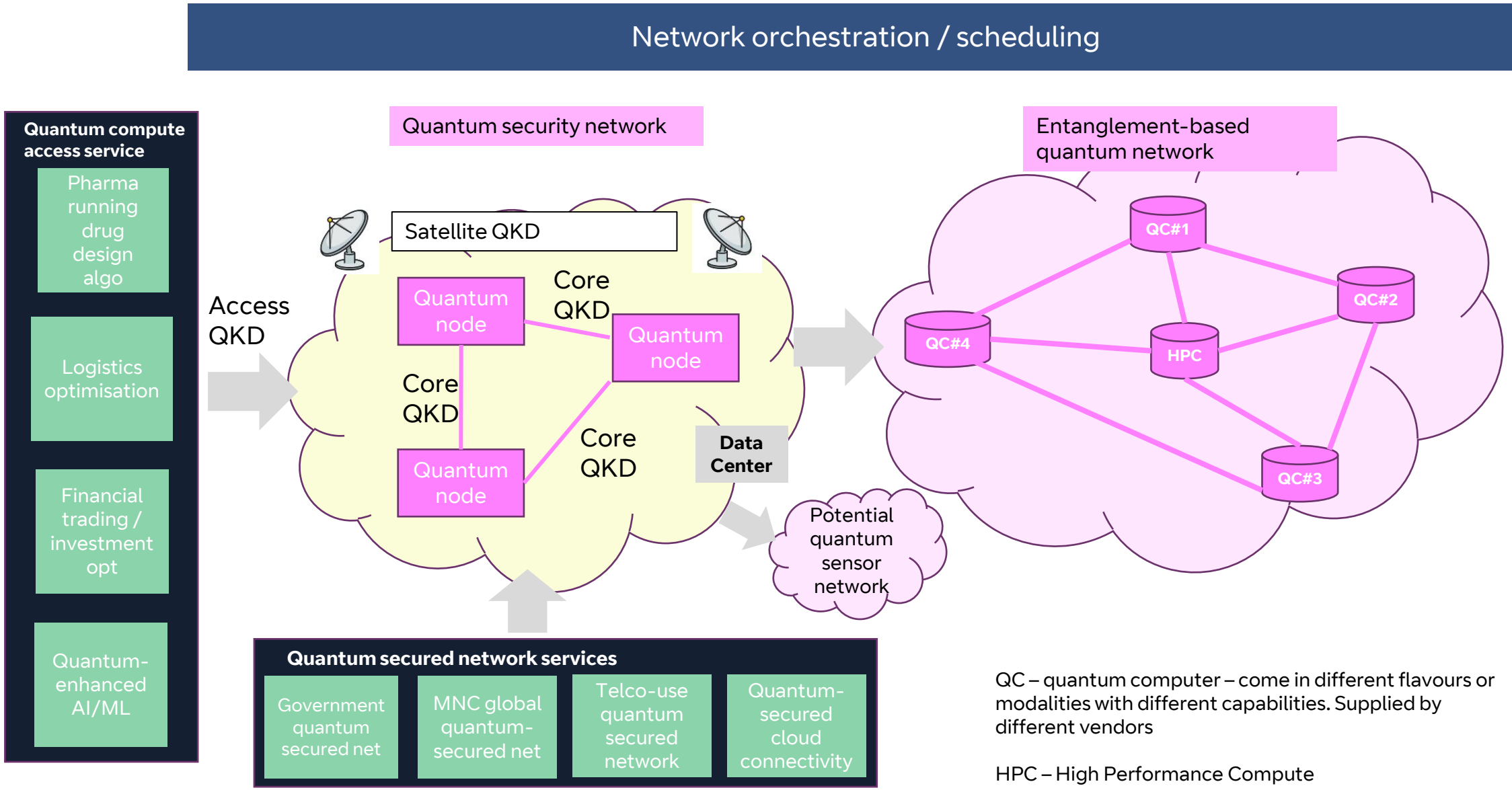
Ultimate quantum network…





- Secure connections between business sites (could be local, regional, national or international)
- Secure back-up to the cloud / DC
- Beyond the access network, connections share fibres
- Metro and Core networks comprise fibres with multiple wavelengths
- IP routers usually used for packet layer traffic networking

Future Quantum Network – 10 year vision



QC – quantum computer – come in different flavours or modalities with different capabilities. Supplied by different vendors

HPC – High Performance Compute

UK Government Ambitions – Autumn 2023 Statement

£2.5bn over 10 years

5 missions identified

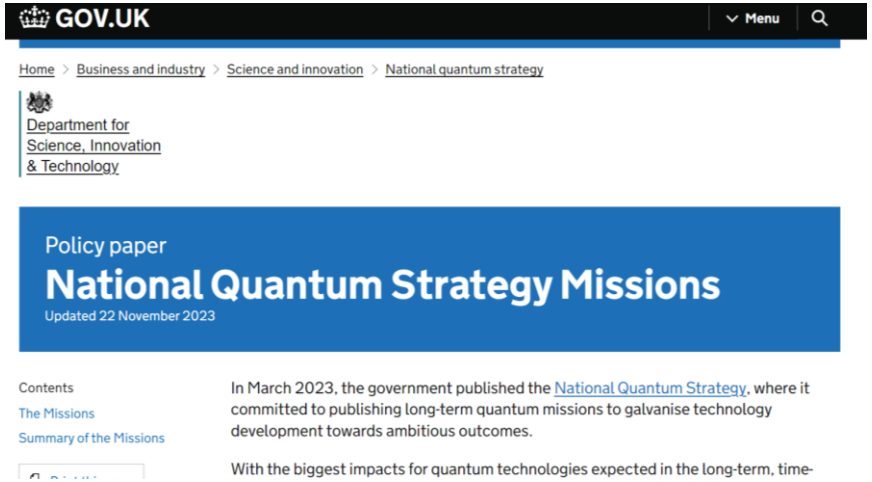
- Quantum computers, networks, sensors, navigation, situational awareness / timing

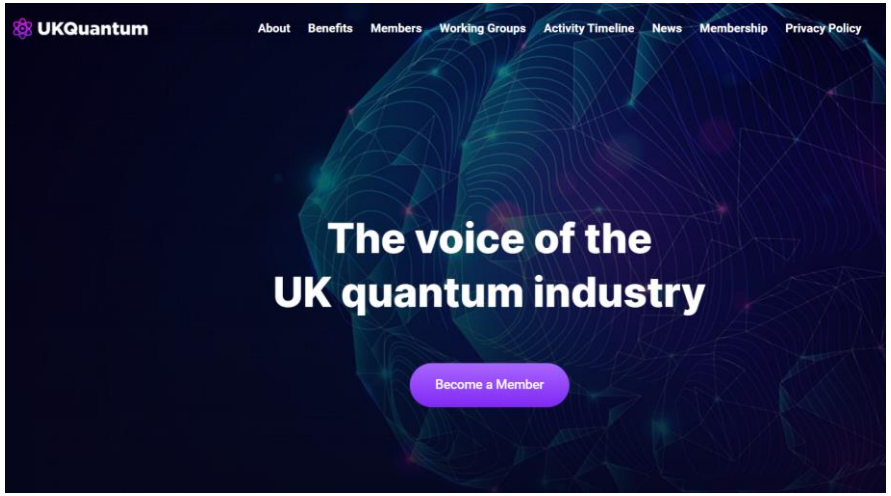
Mission 2: Build the world's most advanced quantum network by 2035

- Interconnect quantum computers
- Nationwide connectivity
- Early commercialisation
- Strategic international collaboration
- Future Quantum Internet

Current Status:

- Next generation of university-led quantum hubs to be announced shortly
- A range of initiatives under discussion to assist UK industry in converting quantum technology into commercial products and solutions
- Recently formed UKQuantum – a body representing quantum industry in the UK
- UK has a promising, if fledgling quantum eco-system





UK Quantum Missions

£1 billion invested since 2014

National Quantum Strategy (publishing.service.gov.uk)

Mission 1 - 2035, … accessible, UK-based quantum computers… across key sectors of the economy.

Mission 2 - 2035, the UK will have deployed the world's most **advanced quantum network at scale, pioneering the future quantum internet.**

Mission 3 - 2030, every NHS Trust will benefit from **quantum sensing-enabled solutions**.

Mission 4 - 2030, **quantum navigation, including clocks**, deployed on aircraft, providing next-generation accuracy independent of satellite signals.

Mission 5 - 2030, mobile, **networked quantum sensors will** be exploited across **critical infrastructure in transport, telecoms, energy, and defense**.

Other global quantum networks

China has the largest with >700 terrestrial fibre QKD links

- Backbone and metro QKD networks
- 2 QKD satellite-ground connections
- They claim > 150 users

South Korea Telecom has a QKD-secured 5G backhaul network, begun in 2016

- Including 330km link (Seoul-Daejeon-Daegu)
- They use Quantum Random Number Generators to assist mobile subscriber authentication
- They have bought a QKD vendor (ID-Quantique)

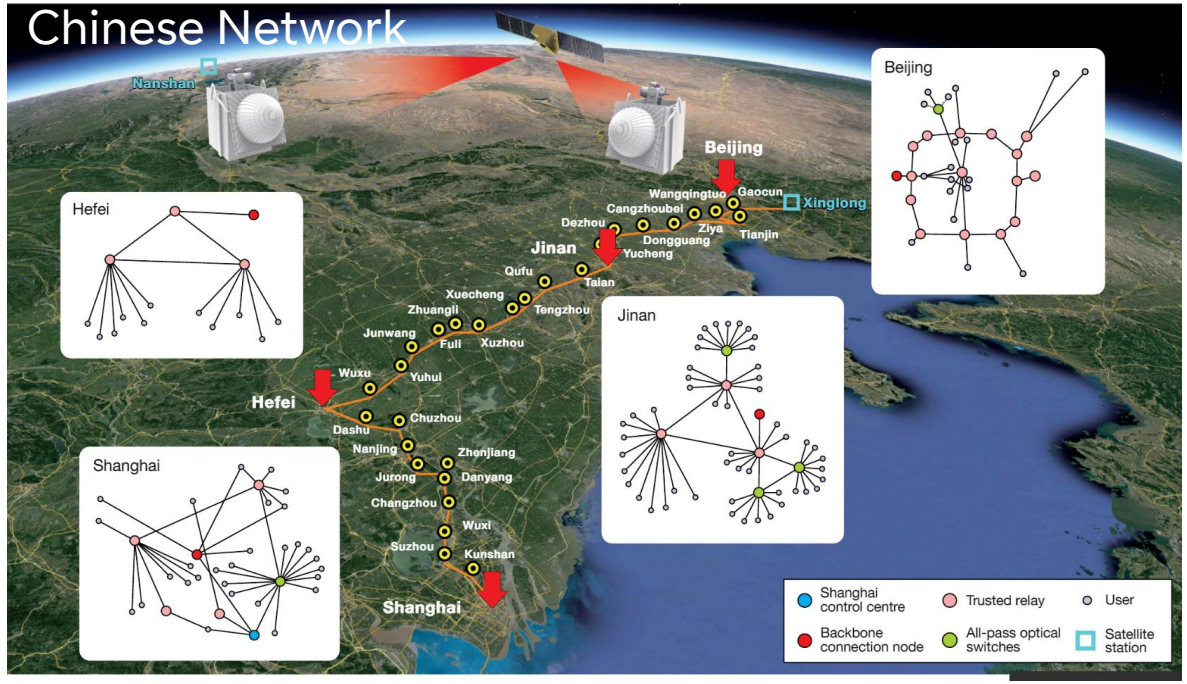
Europe is building 18 national quantum networks

- Known as Euro Quantum Comms Infrastructure (QCI)
- With inter-linking pan-EU net managed by DT
- Heavily subsidised by EU
- UK EXCLUDED from this activity due to BREXIT

Singapore recently announced national QKD plans

- Called National Quantum-Safe Network Plus (NQSN+)
- Launched mid 2024
- To include QKD and PQC

Plus significant activities in US, Japan…



18th March 2019

SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies

- SK Telecom applied Quantum Random Number Generator (QRNG) to the subscriber authentication center of its 5G network
- SK Telecom plans to apply Quantum Key Distribution (QKD) technology to the Seoul-Daejeon section of its LTE and 5G networks to prevent hacking and eavesdropping
- SK Telecom is playing a pivotal role in global standardization of QKD and QRNG technologies at ITU-T.

AIRQKD

An Innovate-UK BT-led project to develop quantum over free space

Objectives –

Free Space Optics 100-200m

QKD over FSO

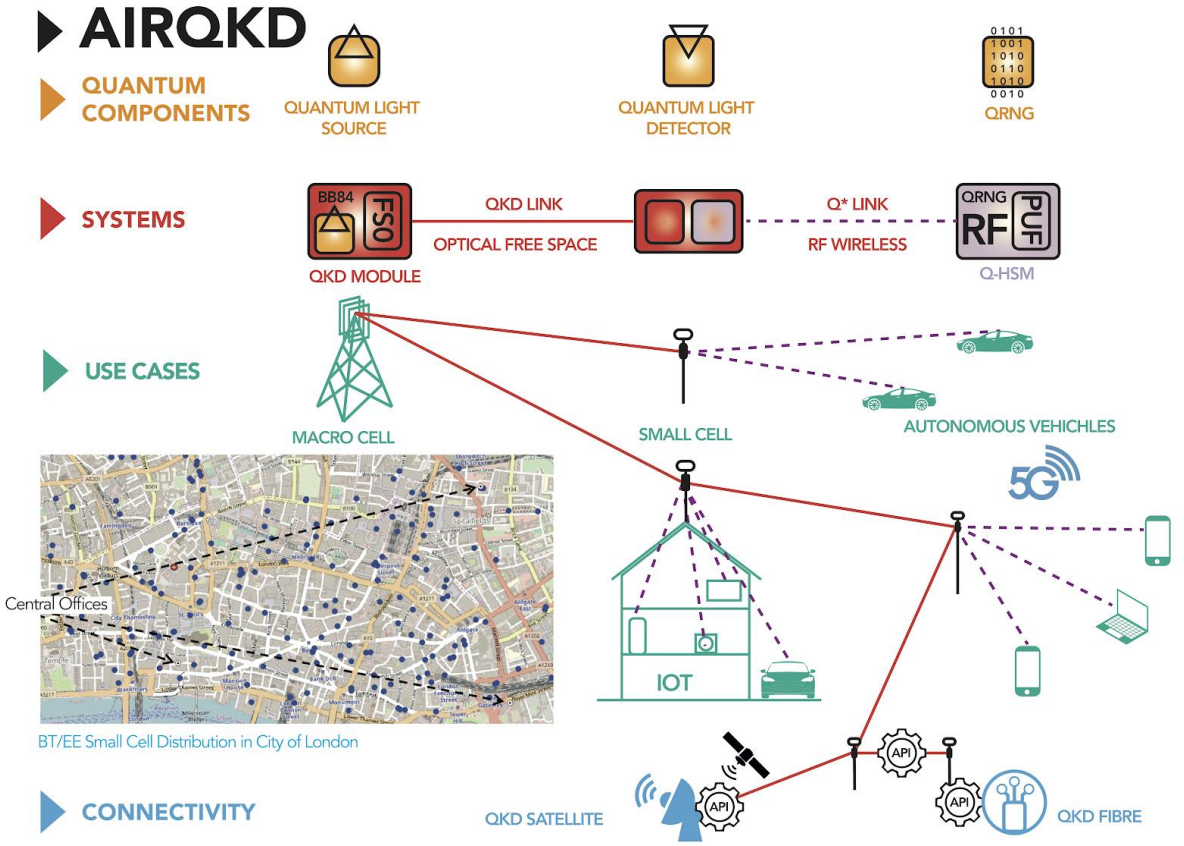
Use cases including autonomous vehicle control, 5G connectivity etc

Edge device security – PUFs

End to end network coordination / control

Large number of partners including

Bay photonics, Fraunhofer, OpenLightComm, NuQuantum, Duality, Angoka, NPL, ArQit, Catapult, and Warwick, Heriot Watt, Bristol, Edinburgh, Strathclyde Unis



Quantum Data Centre of the Future (QDCF)

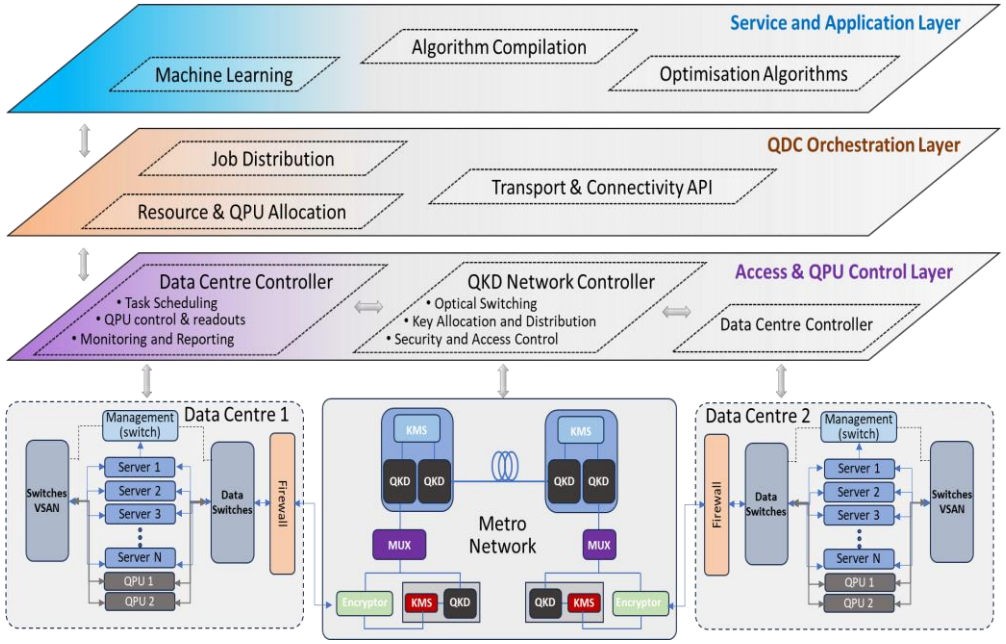
Motivation

- Quantum computers & communications need integration in Quantum Data Centres
- Quantum internet will need classical internet, servers, exchanges and data infrastructure
- Photons for Quantum: 1) Photons are good carriers of quantum information, 2) Easy to produce and manipulate, 3) Easy to transport, high connectivity and scalability, 4) Fast, 5) Many degrees of freedom, 6) Operate at room temperature, 7) No decoherence

Objectives

- A blueprint for a quantum/classical hybrid data centre;
- Data-centre compliant, photonic and optical fibre-based quantum computing modules;
- Quantum communication modules comprising QKD and PQC, to secure inter and intra data centre links;
- A demonstration of a quantum/classical hybrid data centre, within a data centre environment.

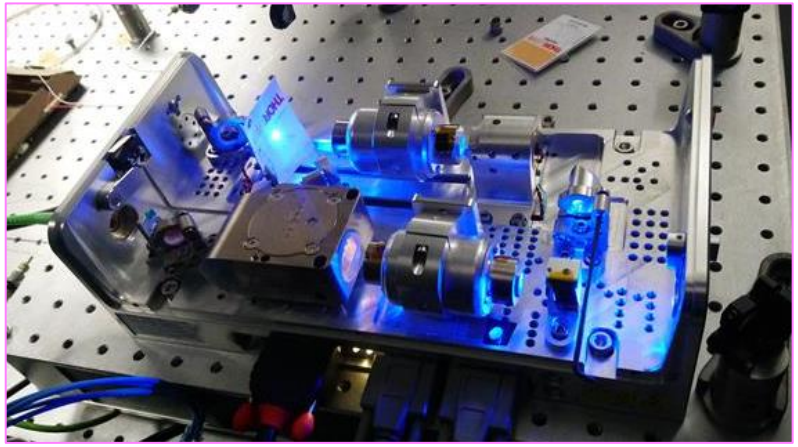
QDCF Quantum Data Centre Architecture

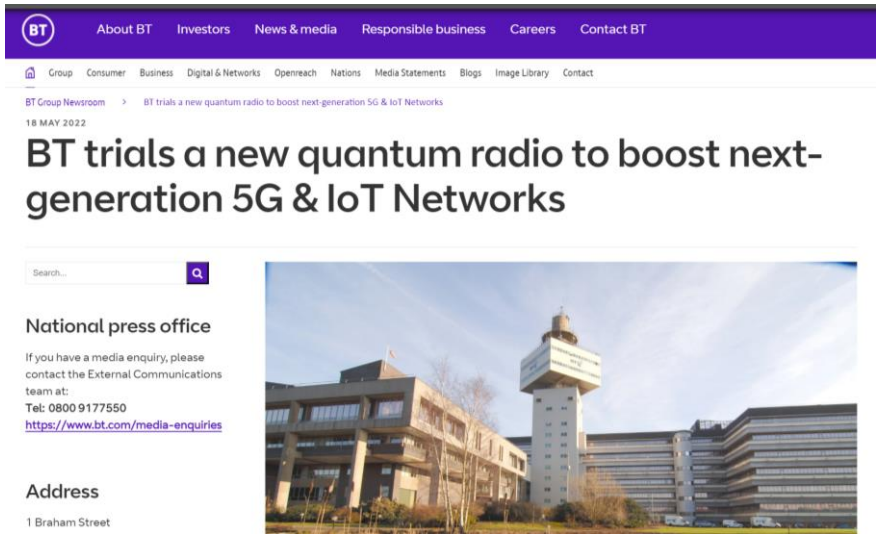


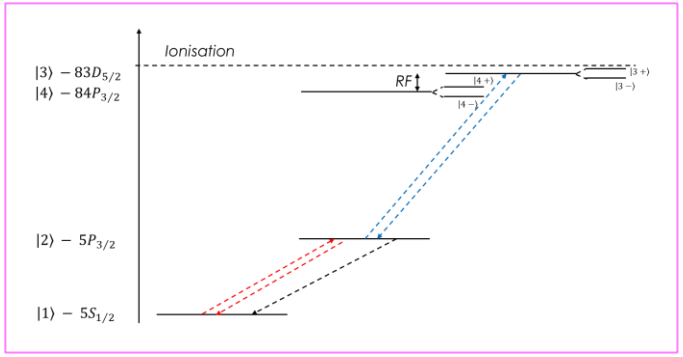
Rydberg atom radio

- We prepare a **vapour** of **excited Rubidium (Rb)** atoms using lasers, exciting **unpaired outer electrons**
- This atomic state is **long lived**, and **sensitive to radio frequency waves** (i.e. 5G signals)…
- This **energy distortion** disturbs the **electromagnetically induced transparency** of the **atomic system,** and is measurable at a photodiode.

Room temperature vapour cell

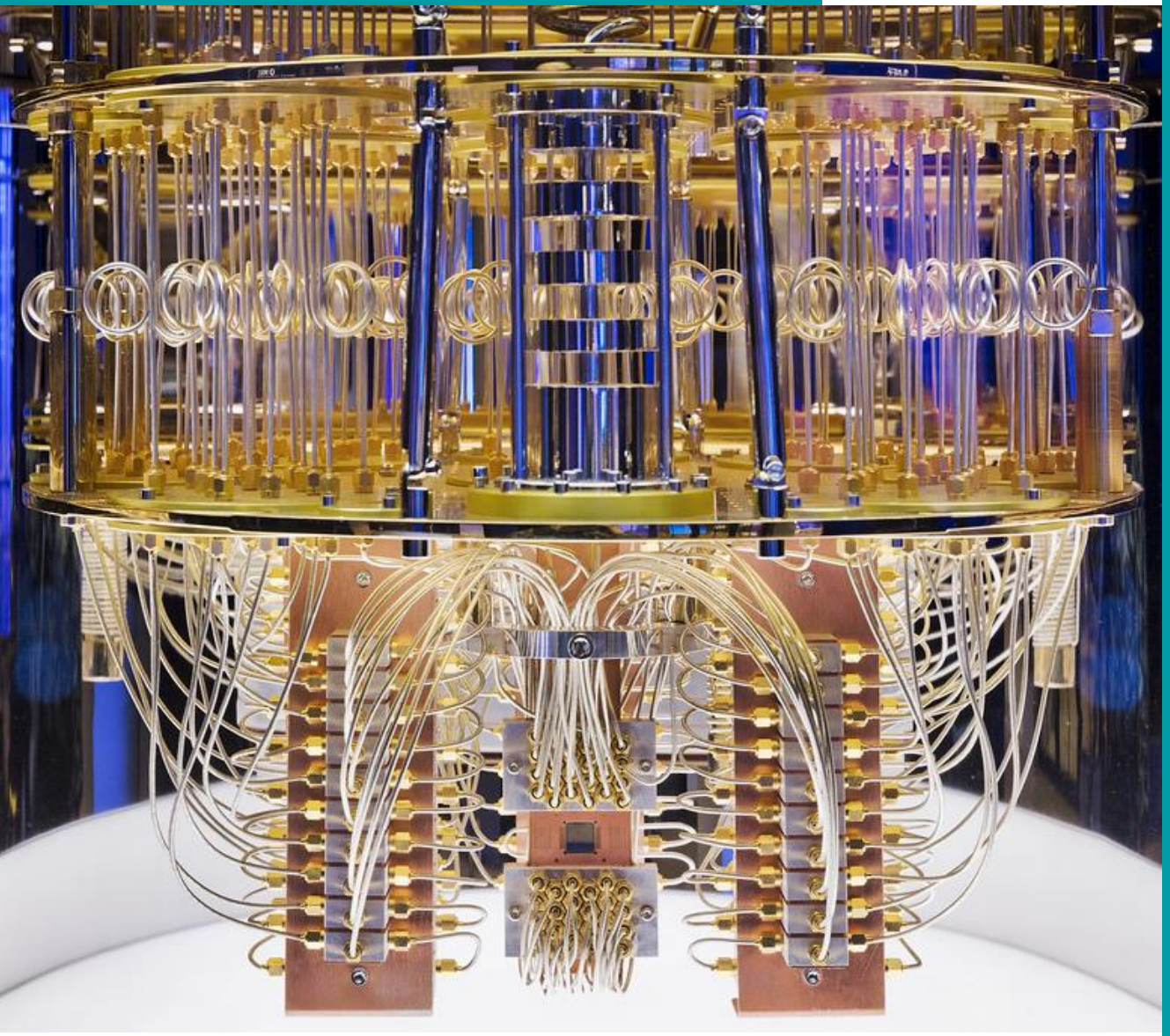






Free Electron energy level diagram

To conclude – a few comments on…



Quantum Computers

Quantum Processing might offer:

- Better optimizations
- Faster time-to-solution
- Maybe energy savings in the calculation?

A coprocessor to classical – very strong at certain tasks, but not others.

Can Near Term Quantum Computers help with Real World Optimisation and Constraint Satisfaction Problems ?

Microphysical Layer & Abstract Problems
LDPC Error correction for Optical or Wireless Data Transmission
MIMO Decoding
Antenna Design
Abstract graph search – identification of clusters of anomalous connectivity/activity

Well characterised problems,

Few unknown unknowns

- Uncertainties in physical aspects
e.g. noise model, loss model

Macro-Physical Layer Problems
Frequency of Uplift
Network resilience
Placement of security components such as Firewalls
Placement of content distribution nodes

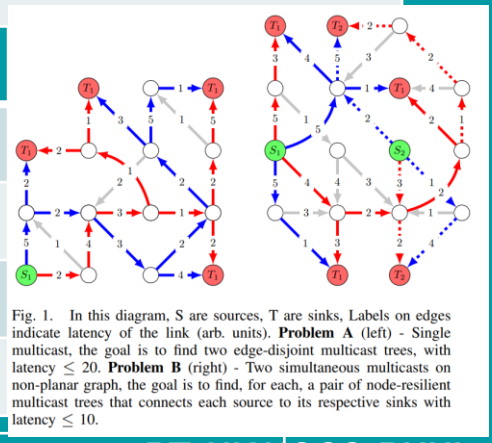


Fig. 1. In this diagram, S are sources, T are sinks, Labels on edges indicate latency of the link (arb. units). **Problem A** (left) - Single multicast, the goal is to find two edge-disjoint multicast trees, with latency ≤ 20. **Problem B** (right) - Two simultaneous multicasts on non-planar graph, the goal is to find, for each, a pair of node-resilient multicast trees that connects each source to its respective sinks with latency ≤ 10.

Human Leyer Problems
Field Force Optimisation – allocation of jobs to engineers
Location of service hubs
Geographic ordering of jobs
Predictive placement of content to CDNs

NISQTI Innovate UK Feasibility Study

BT, UK NQCC, RHUL

Innovate UK

PHASECRAFT

THE QUANTUM ALGORITHMS COMPANY

rigetti

QUANTUM COMPUTING

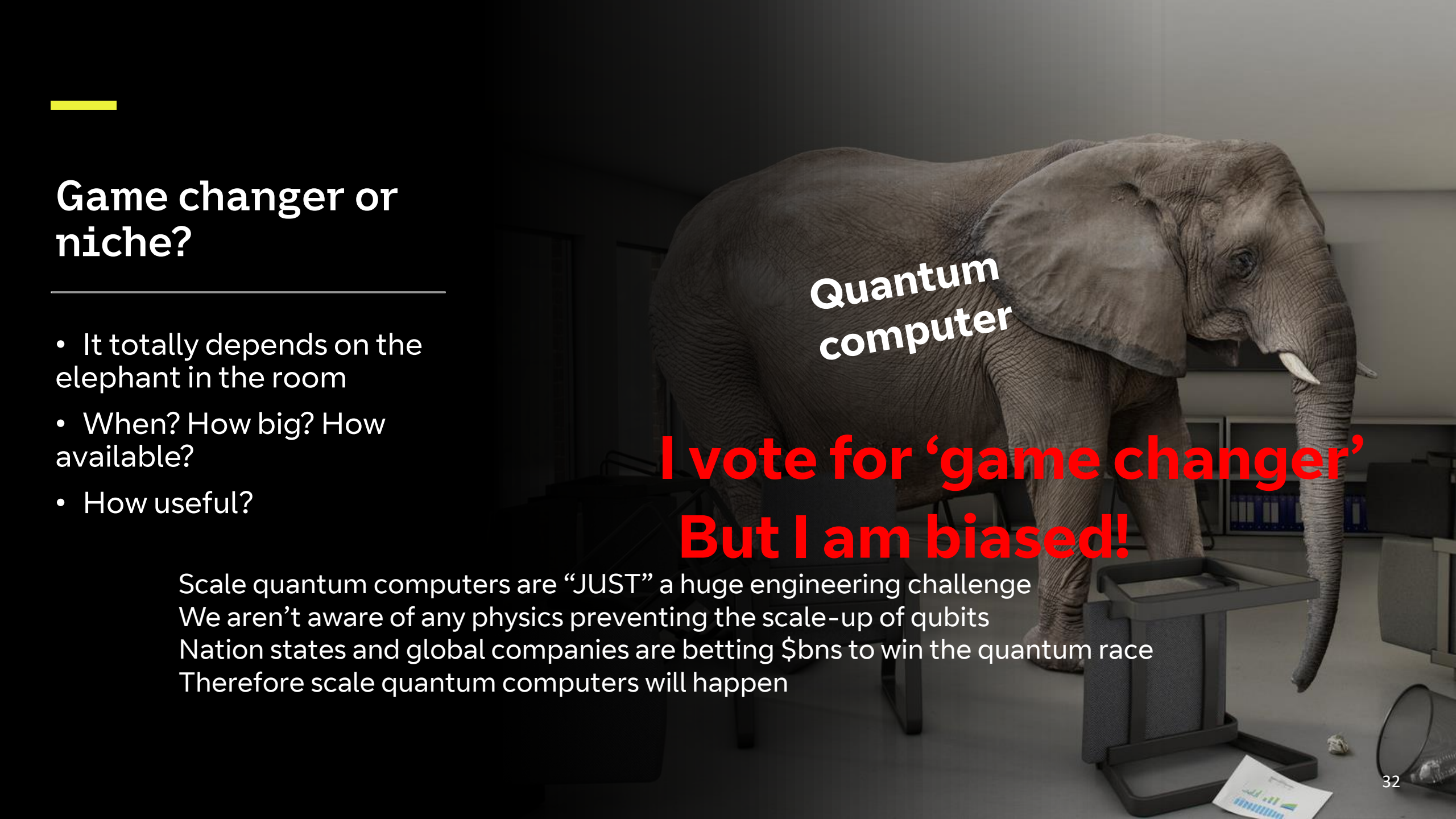
Early signs of possible advantages to warm-start classical solvers for certain problems

Conclusions

- **Quantum is coming**… Quantum Communications, Quantum Computing & Quantum Sensing.
- **Quantum Computers** are the big-ticket items, promising vast compute power increase
- **Quantum communications** initially will provide an ultra-secure communications infrastructure where needed (working closely with other cryptography approaches)
- **Quantum networks** will ultimately interconnect quantum devices, heralding a quantum internet
- **Multiple other quantum benefits coming** including ultra precise quantum clocks, ultra sensitive quantum sensors and imaging

Game changer or niche?

- It totally depends on the elephant in the room
- When? How big? How available?
- How useful?



I vote for 'game changer'
But I am biased!

Scale quantum computers are "JUST" a huge engineering challenge
We aren't aware of any physics preventing the scale-up of qubits
Nation states and global companies are betting $bns to win the quantum race
Therefore scale quantum computers will happen

The Institution of Engineering and Technology

Thank you for your attendance

The following upcoming talks have been secured in our IET ACLN 2024 programme. Please check our IET EngX website for more details of our events and how to register:
https://engx.theiet.org/local-networks/ea1

Visit to BT's Robotics & Drone Lab: BT Applied Research Facility, Adastral Park, Ipswich
[05 June 2024, 6:30pm, Evening Excursion]

New Space, the future of satellite communications, Prof. Andy Sutton, BT Fellow & Principal Network Architect
[18 July 2024, 7pm, HYBRID]

Routes to Registration: IET Registration & Standards Support Unit (RSSU)
[26 Sept 2024, 6pm, ONLINE ONLY]

[HYBRID] events normally run from The Atrium, University of Suffolk, Ipswich and via Microsoft Teams.

For more details and how to register please visit: https://engx.theiet.org/local-networks/ea1

CPD Certificates for today's and previous Anglian Coastal Local Network talks can be found on this site.