Quantum Cyber Security
The landscape and Challenges

Elham Kashefi

University of Edinburgh
CNRS, Sorbonne University
National Quantum Computing Center

Big Data Machine

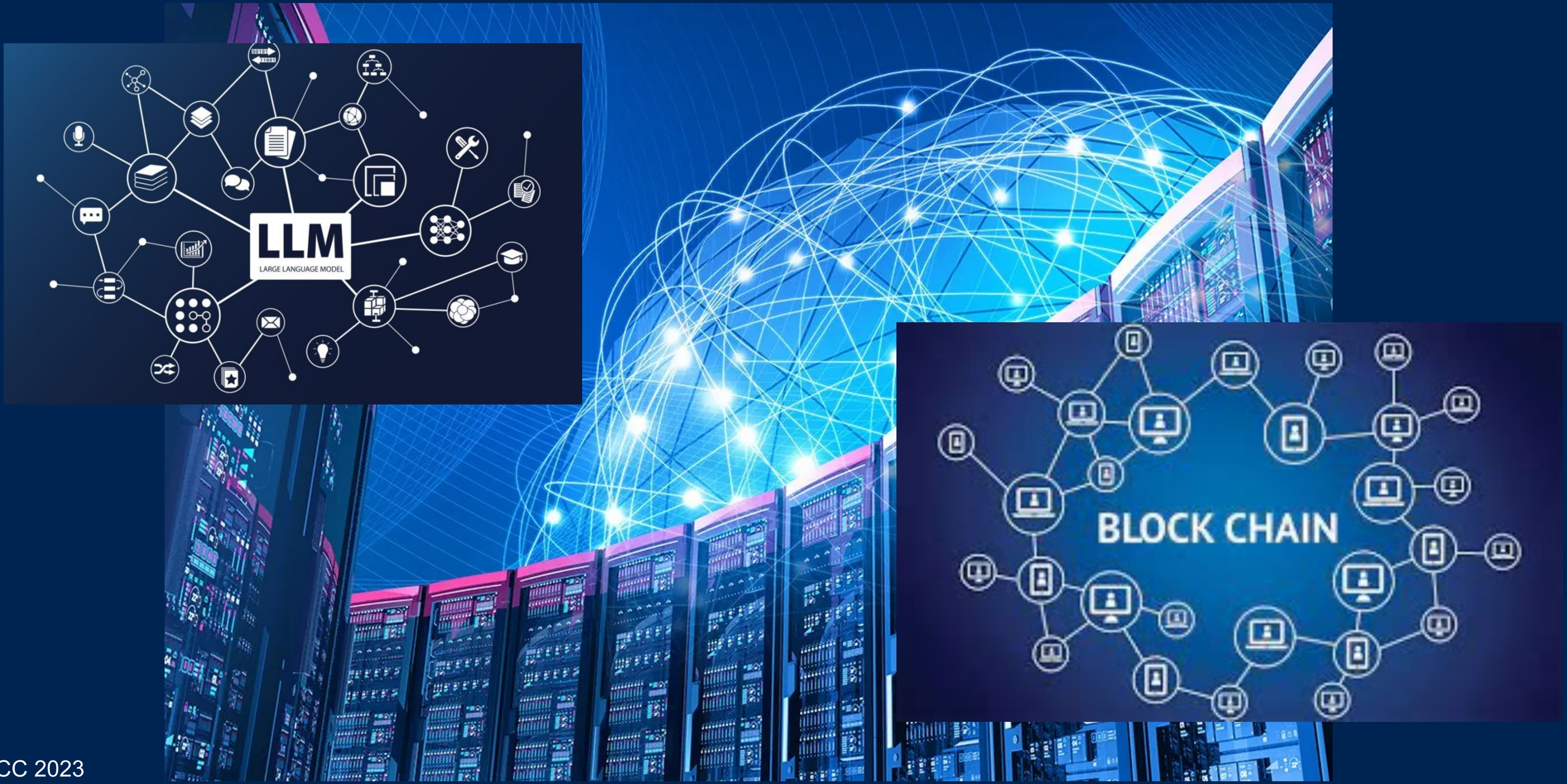
Collection/Correlation/Communication/Trading

Big Data Machine

Collection/Correlation/Communication/Trading

Big Data Machine

Collection/Correlation/Communication/Trading



Big Data Machine

Collection/Correlation/Communication/Trading

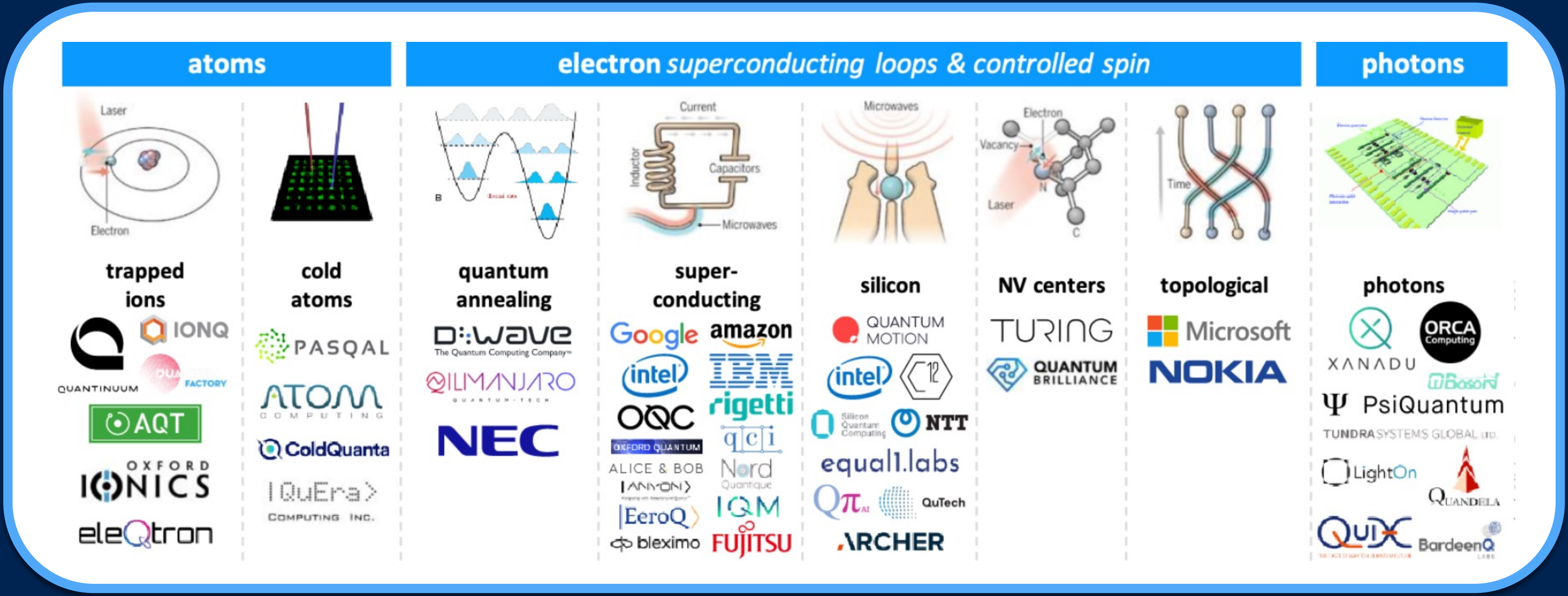
Fast Massive Secure Accurate Data Machine

will

consume the energy of the planet

Breaking the Barrier

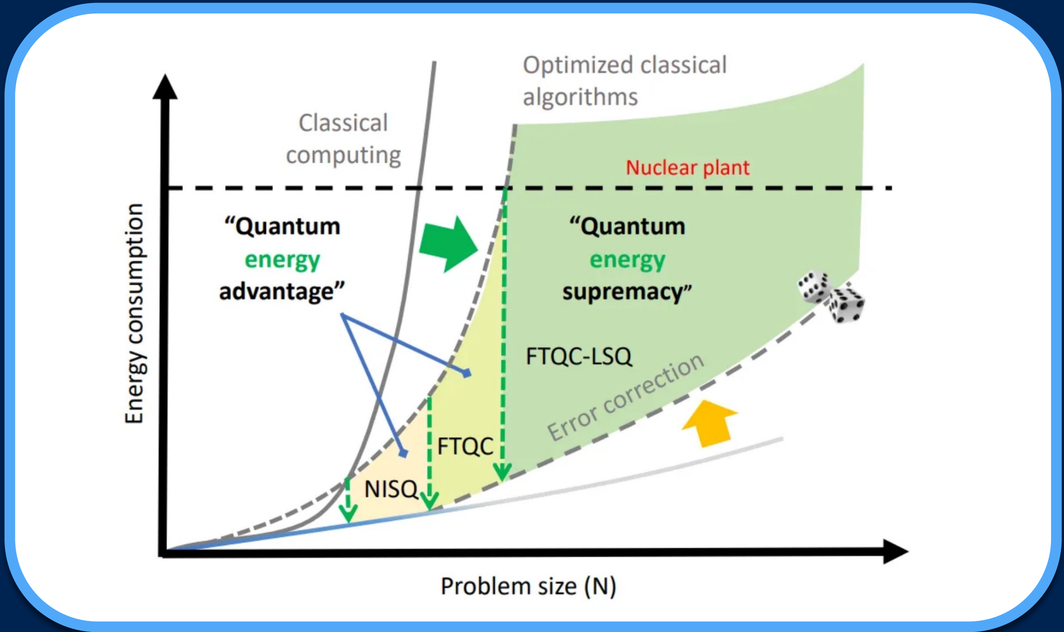
Speed



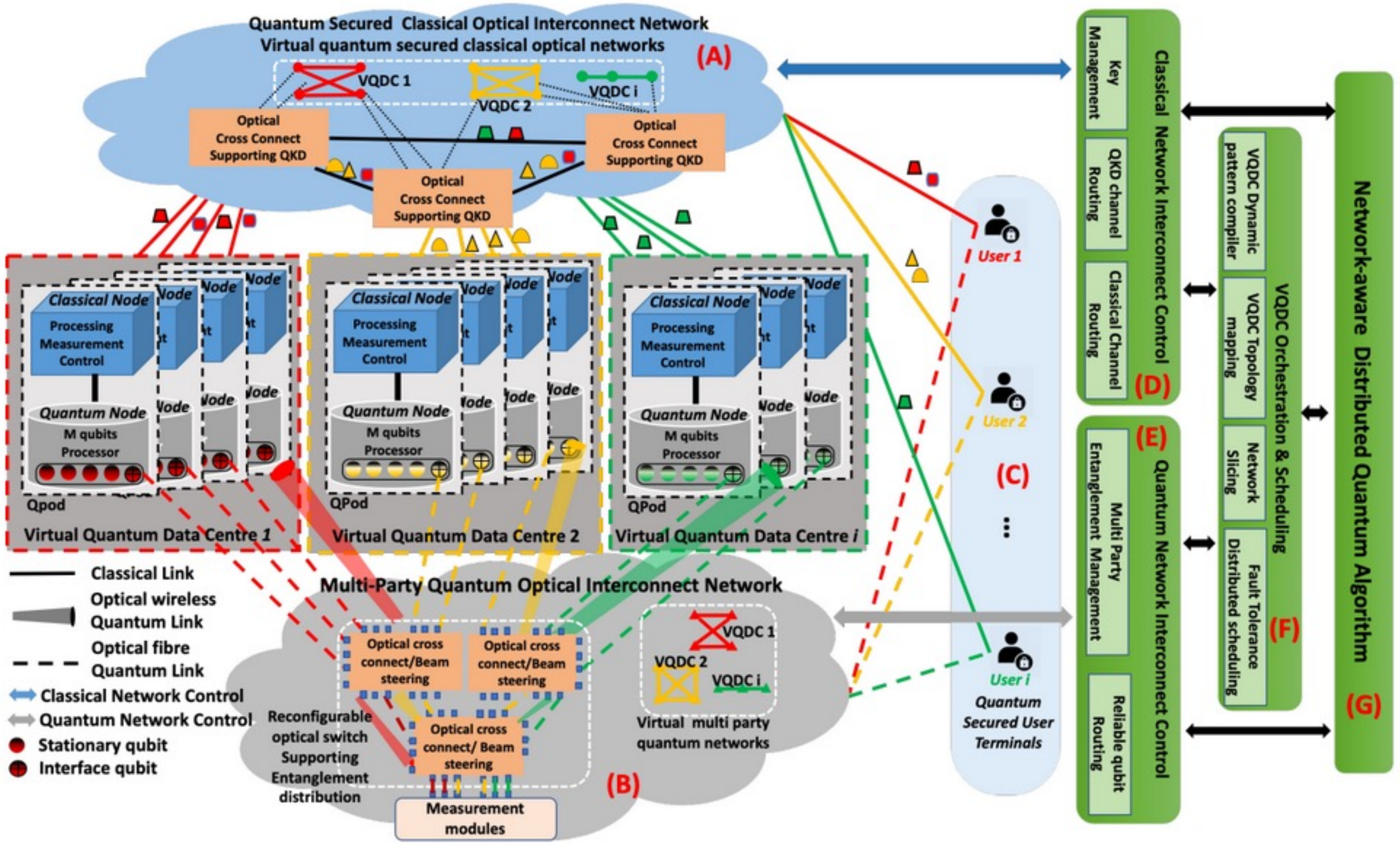
Security

quantum keys QKD / BB84
protects symetric keys with optical link (fiber or sat)
Quintessence Labs
NANO-META TECHNOLOGIES, INC.
Q→NU
KEEQUANT
KETS
国盾量子 QuantumCTek
QRATE QUANTUM COMMUNICATIONS
asky
QuantLR
循态量子 XT Quantech
Qubitekk
ciena
S-FIFTEEN SPACE SYSTEMS QUANTUM-SAFE COMMUNICATION
SAMSUNG
TOSHIBA
IDQ
Qunnect
QUANTUM XCHANGE
Crypta Labs
ANAMETRIC
Qubit Reset
infotecs
QUSIDE
ArQit
MagiQ
nu QUANTUM
QEYnet
Mt Pelerin
SMARTS
AegiQ

Energy



Future Secure Fast Networked Quantum Data Machine For Public Good


Quantum Secured Classical Optical Interconnect Network
Virtual quantum secured classical optical networks
(A)
VQDC 1
VQDC 2
VQDC i
Optical Cross Connect Supporting QKD
Optical Cross Connect Supporting QKD
Optical Cross Connect Supporting QKD
Classical Node
Processing Measurement Control
Quantum Node
M qubits Processor
Qpod
Virtual Quantum Data Centre 1
Classical Node
Processing Measurement Control
Quantum Node
M qubits Processor
QPod
Virtual Quantum Data Centre 2
Classical Node
Processing Measurement Control
Quantum Node
M qubits Processor
QPod
Virtual Quantum Data Centre i
Classical Link
Optical wireless Quantum Link
Optical fibre Quantum Link
Classical Network Control
Quantum Network Control
Stationary qubit
Interface qubit
Multi-Party Quantum Optical Interconnect Network
Optical cross connect/Beam steering
Optical cross connect/Beam steering
Optical cross connect/ Beam steering
Reconfigurable optical switch Supporting Entanglement distribution
Measurement modules
(B)
VQDC 1
VQDC 2
VQDC i
Virtual multi party quantum networks
User 1
User 2
(C)
⋮
User i
Quantum Secured User Terminals
Classical Network Interconnect Control
Key Management
QKD channel Routing
Classical Channel Routing
(D)
(E)
Quantum Network Interconnect Control
Multi Party Entanglement Management
Reliable qubit Routing
VQDC Orchestration & Scheduling
VQDC Dynamic pattern compiler
VQDC Topology mapping
Network Slicing
Fault Tolerance Distributed scheduling
(F)
Network-aware Distributed Quantum Algorithm
(G)

Net Zero - Health - Fraud Detection

Regulated Computing - Privacy Preserving

Quantum Computer

Manipulate in a programmable, fully controllable and flexible way quantum information

- Can perform more (types) of operations
- Many problems can be solved exponentially faster
- Vast possibilities from optimisation, machine learning, inventing new materials, medicines to energy, but ...
- Could be a serious threat for Cyber Security!

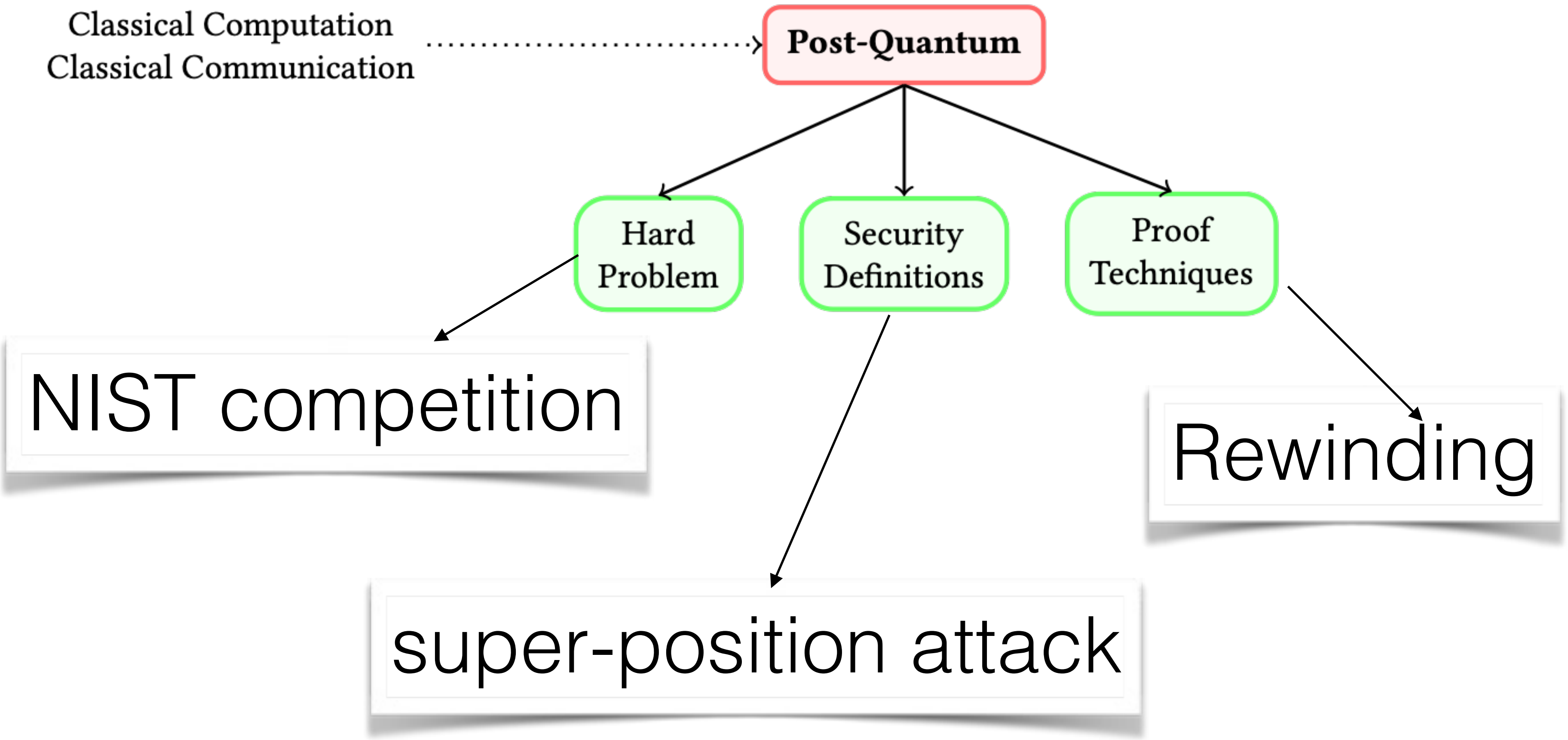
The Quantum Cyber Security Landscape

> every impact of the development of quantum technologies on the security and privacy of communications and computations

Disruptive and New opportunities

Wallden and Kashefi, Communications of the ACM

Good Guys Capacity



Classical Computation
Classical Communication

Post-Quantum

Hard Problem

Security Definitions

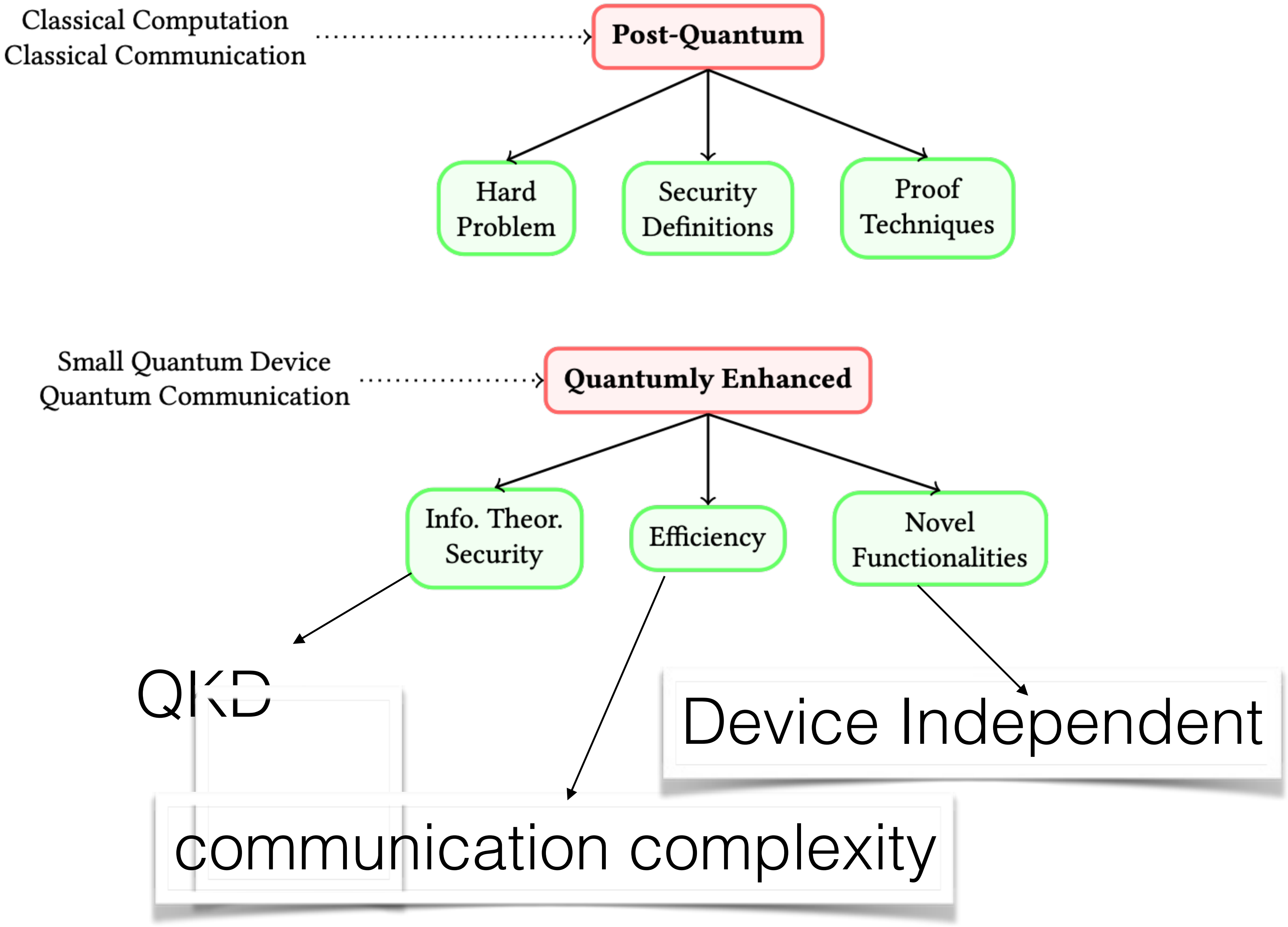
Proof Techniques

NIST competition

super-position attack

Rewinding

Good Guys Capacity



Classical Computation
Classical Communication

Post-Quantum

Hard Problem

Security Definitions

Proof Techniques

Small Quantum Device
Quantum Communication

Quantumly Enhanced

Info. Theor. Security

Efficiency

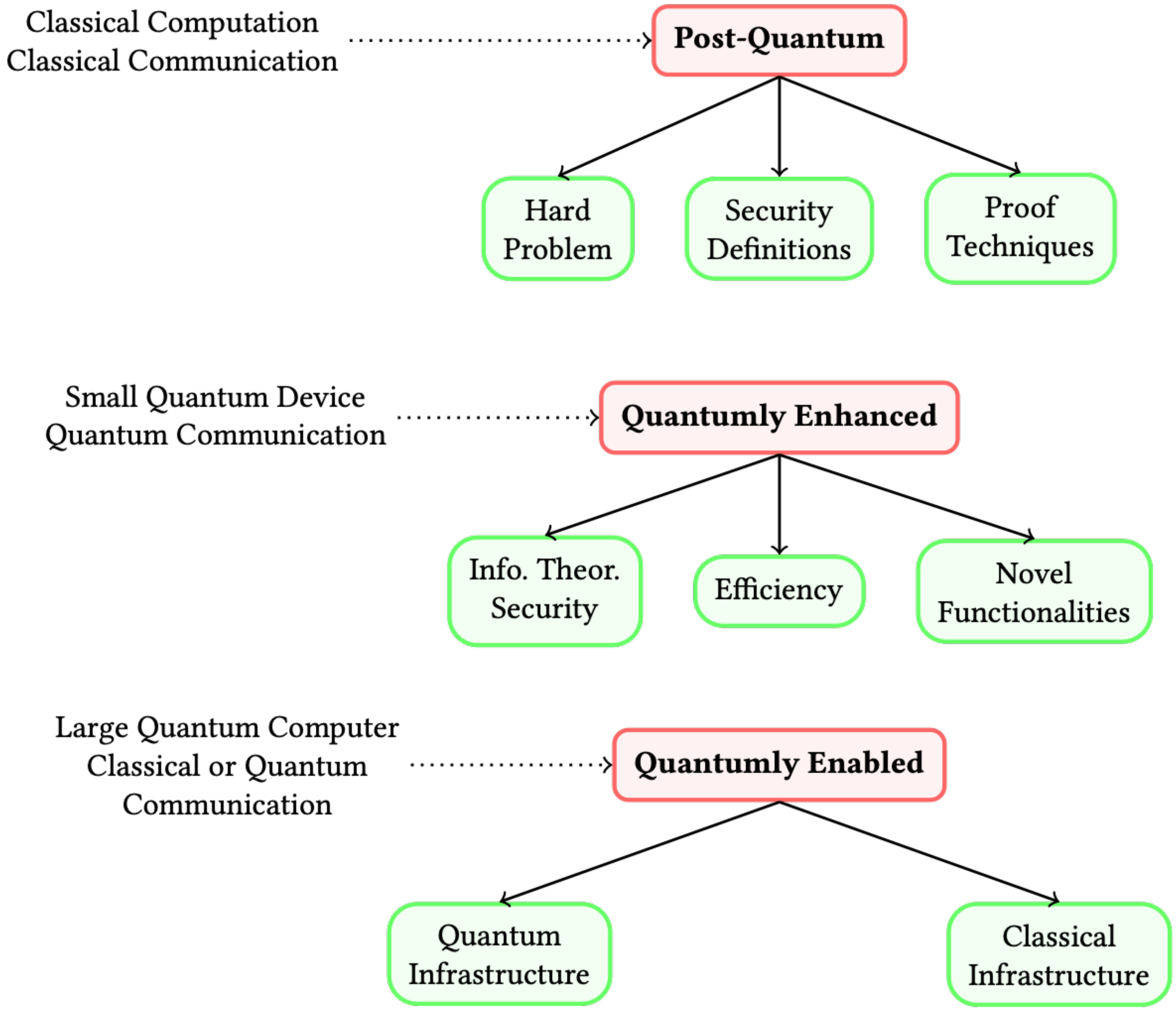
Novel Functionalities

QKD

communication complexity

Device Independent

Good Guys Capacity



Classical Computation
Classical Communication

Post-Quantum

Hard Problem

Security Definitions

Proof Techniques

Small Quantum Device
Quantum Communication

Quantumly Enhanced

Info. Theor. Security

Efficiency

Novel Functionalities

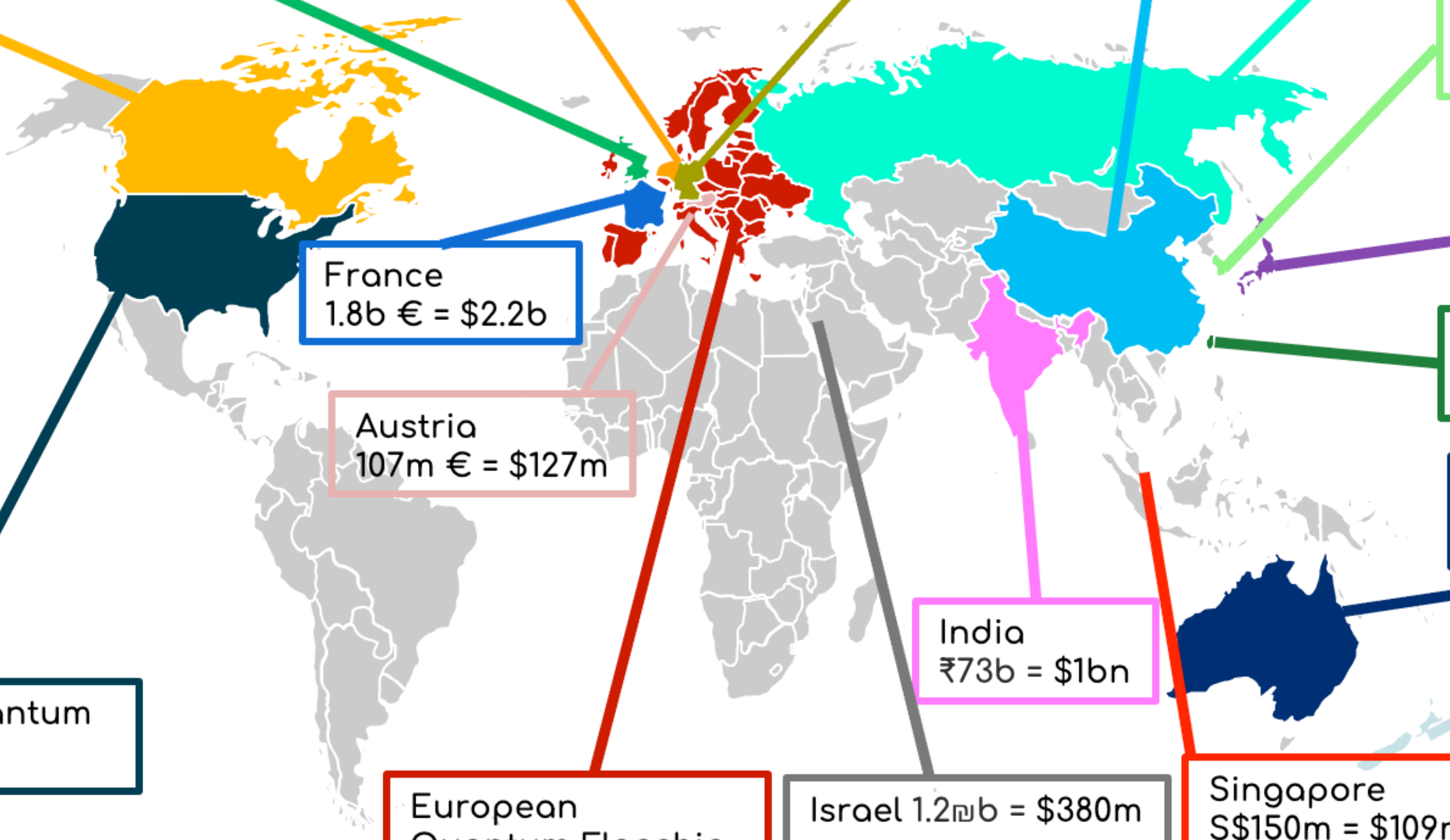
Large Quantum Computer
Classical or Quantum Communication

Quantumly Enabled

Quantum Infrastructure

Classical Infrastructure

Quantum effort worldwide



Global effort 2021 $24.4b (estimate)

Quantum Canada
CA$1.36b = $1.1b

United Kingdom
£1b = $1.3b

Netherlands
765m € = $904m

Germany
2.6b € = $3.1b

China
$10b

Russia
₽50b = $663m

South Korea
₩44.5b = $37m

Japan
¥50b = $470m

Taiwan
NT$8b = $282m

Australia
AU$130m = $98.5m

New Zealand
$36.75m

France
1.8b € = $2.2b

Austria
107m € = $127m

US National Quantum Initiative $1.2b

European Quantum Flagship
1b € = $1.1b

Israel 1.2₪b = $380m

India
₹73b = $1bn

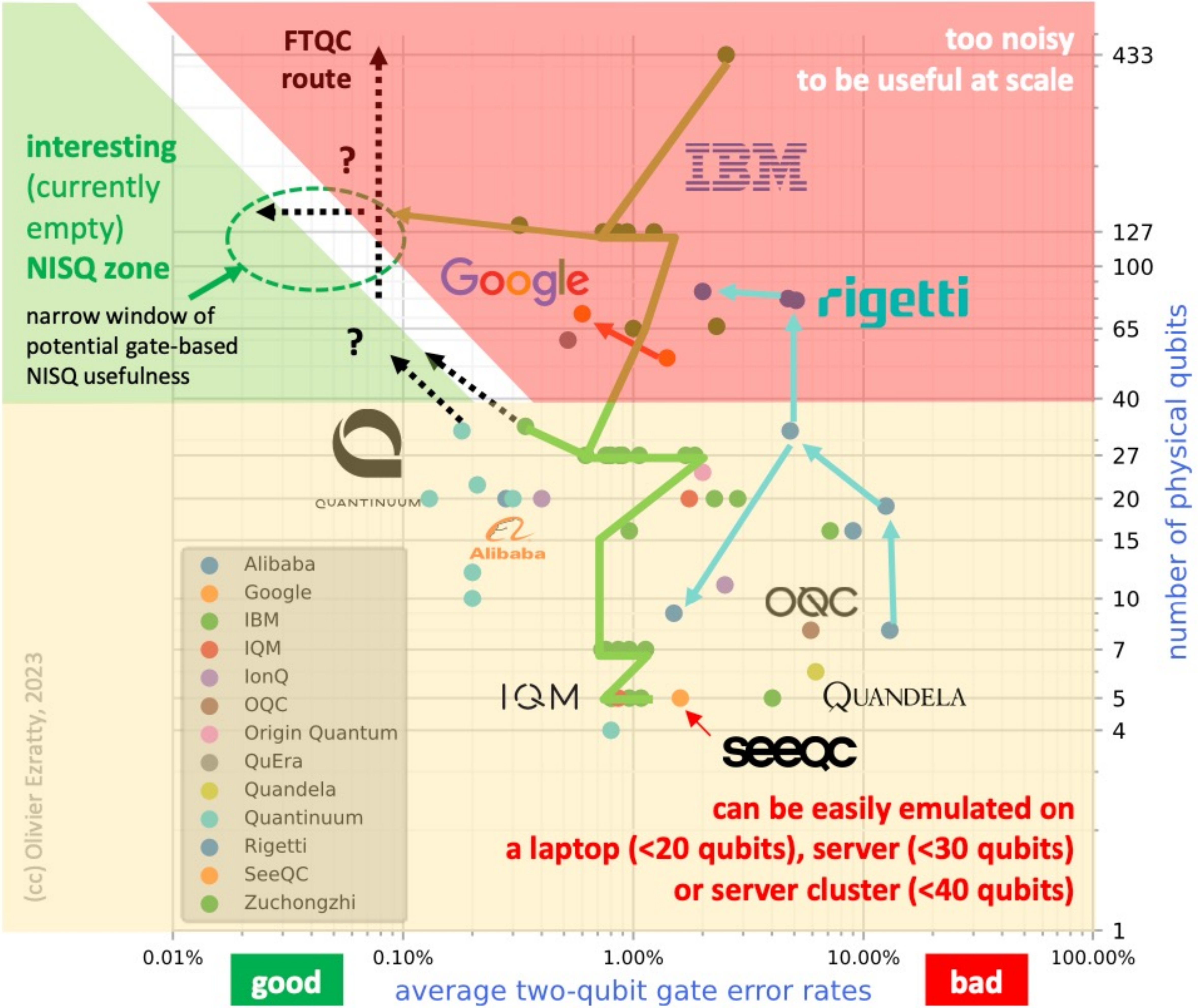
Singapore
S$150m = $109m

dy Matuschak | Anne Broadbent | Anne Canteaut | Anne Matsuura | Anthony Leverrier | Antoine Browaeys | Anton Zeilir
Aram Harrow | Arieh Warshel | Arthur Holly Compton | Arthur Leonard Schawlow | Artur Ekert | Astrid Lambrecht | Auc
enfait | Axel Becke | Benjamin Huard | Benoît Valiron | Bettina Heim | Bob Wiens | Boris Podolsky | Brian Josephson | Br
eisbuch | Clauss Jönsson | Clinton Davisson | Cornelis Dorsman | Craig Gidney | Cristian Calude | Cristina Escoda | Cyril
iche | Damien Stehlé | Daniel Esteve | Daniel Gottesman | Dave Wecker | David Bohm | David Deutsch | David DiVincenz
ishenina | Emanuel Knill | Emmy Noether | Enrico Fermi | Eric Cornell | Ernest Rutherford | Ernst Ising | Erwin Schröding
enne Klein | Ettore Majorana | Ewin Tang | Fabio Sciarrino | Faye Wattleton | Felix Bloch | Francesca Ferlaino | Franck Bales
Frank Wilczek | François Le Gall | Frédéric Grosshans | Frédéric Magniez | Freeman John Dyson | Friedrich Hund | Fried
schen | Geordie Rose | George Uhlenbeck | Georges Paget Thomson | Georges Zweig | Georges-Olivier Reymond | Ger
o | Haig Farris | Hans Albrecht Bethe | Hans Jürgen Briegel | Hantaro Nagaoka | Harald Fritzsch | Hartmut Neven | He
merlingh Onnes | Heinrich Hertz | Hélène Bouchiat | Hélène Perrin | Hendrik Anthony Kramers | Hendrik Casimir | Hen

Understanding Quantum Technologies

Sixth edition – 2023

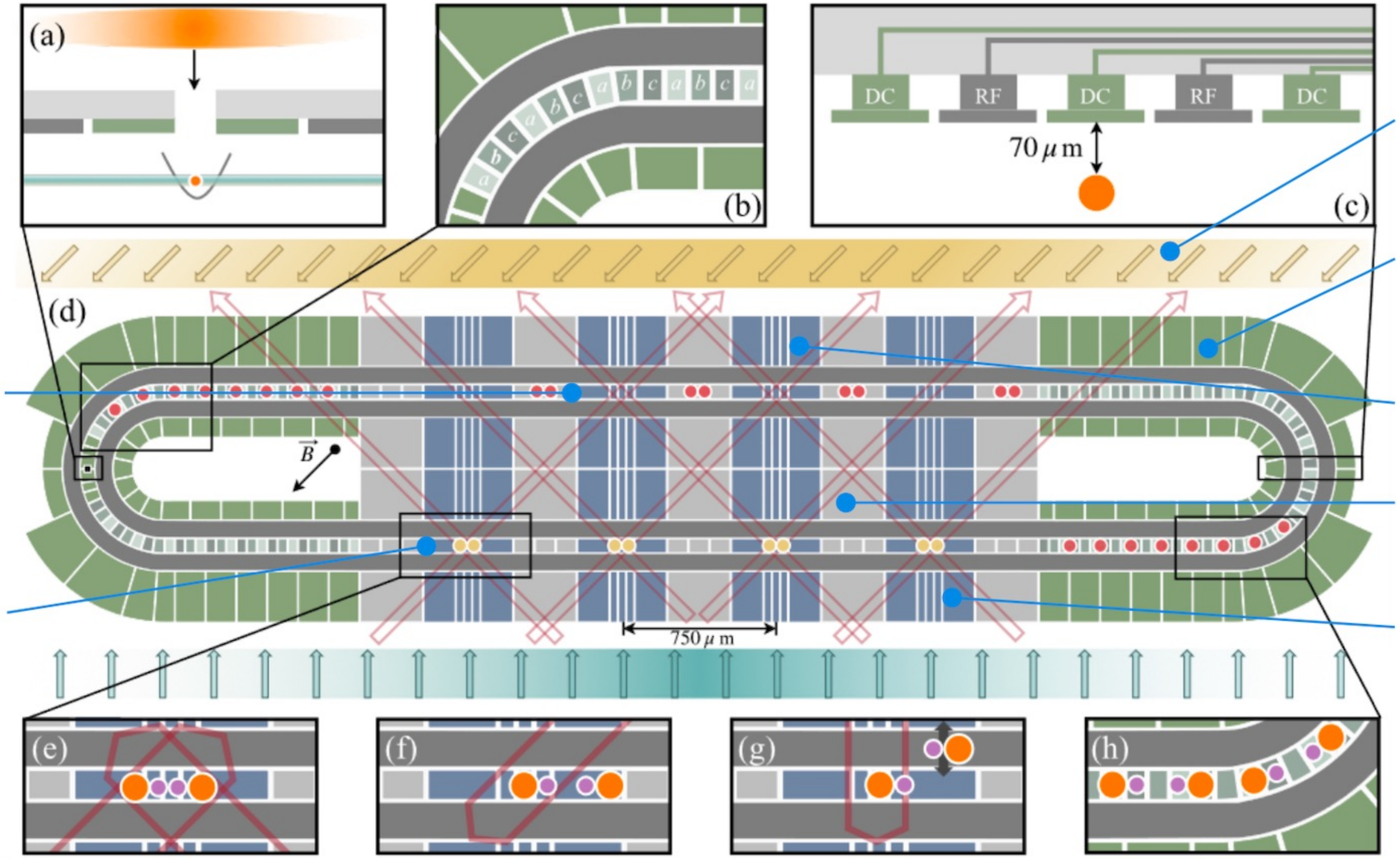
Olivier Ezratty


FTQC
route
too noisy
to be useful at scale
interesting
(currently
empty)
NISQ zone
narrow window of
potential gate-based
NISQ usefulness
?
?
IBM
Google
rigetti
QUANTINUUM
Alibaba
OQC
IQM
QUANDELA
seeqc
can be easily emulated on
a laptop (<20 qubits), server (<30 qubits)
or server cluster (<40 qubits)
Alibaba
Google
IBM
IQM
IonQ
OQC
Origin Quantum
QuEra
Quandela
Quantinuum
Rigetti
SeeQC
Zuchongzhi
(cc) Olivier Ezratty, 2023
433
127
100
65
40
27
20
15
10
7
5
4
1
number of physical qubits
0.01%
0.10%
1.00%
10.00%
100.00%
good
average two-qubit gate error rates
bad

2D MOT produces a collimated beam of atoms, allowing for higher neutral atom density and faster loading than an effusive oven.

abc tiling of electrodes for conveyor belt transport.

RF tunnels to implement inner and outer RF electrodes. Ions are trapped 70 m below the trap surface.



red circles represent qubits sitting in storage during gates (^{138}Ba+ ions are omitted for simplicity).

yellow circles represent qubits that are gated.

yellow arrows indicate the Doppler sheet beam direction while blue arrows indicate the Doppler repump sheet beam direction.

green curved zones are conveyor belt regions for ion storage.

top blue zones are UG01-UG04 gate zones (from right to left), used for sorting but not quantum operations.

grey loops are RF electrodes.

bottom blue zones are DG01-DG04 (from left to right), used for quantum operations.

racetrack size
6.58 mm x 2.02 mm
for 32 qubits

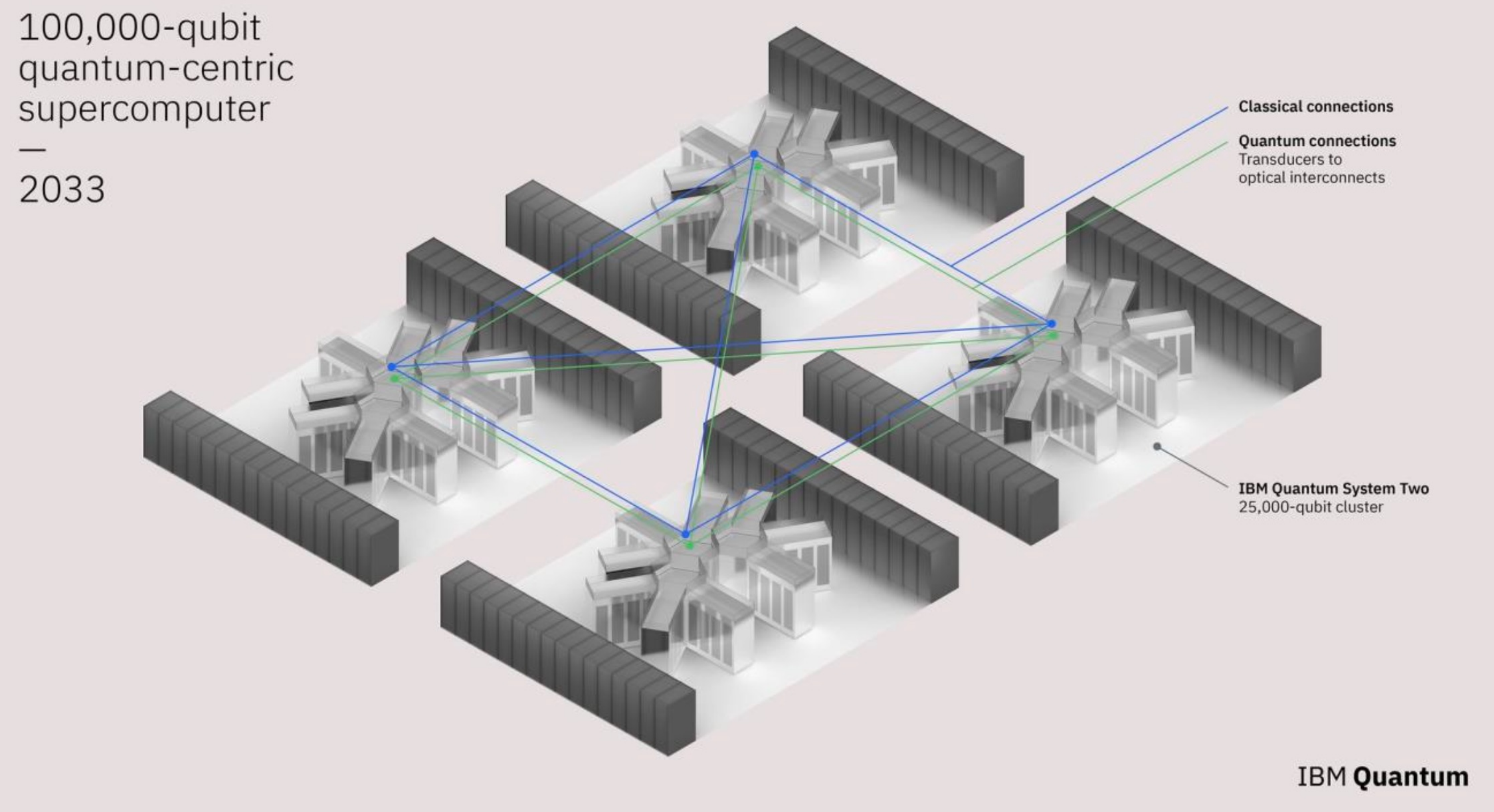
Ion configuration and beam direction for 2Q gates. Large orange circles represent ^{171}Yb+ while smaller purple circles represent ^{138}Ba+.

Ion configuration and beam directions for 1Q gates on left ^{171}Yb+.

Ion configuration and beam directions for state preparation and measurement (SPAM) operations on left ^{171}Yb+ with micromotion hiding on right ^{171}Yb+.

Storage ion configuration in conveyor belt region.

QUANTINUUM



100,000-qubit quantum-centric supercomputer
—
2033

Classical connections

Quantum connections
Transducers to
optical interconnects

IBM Quantum System Two
25,000-qubit cluster

IBM **Quantum**

QUANTUM THREAT TIMELINE REPORT 2023

Authors

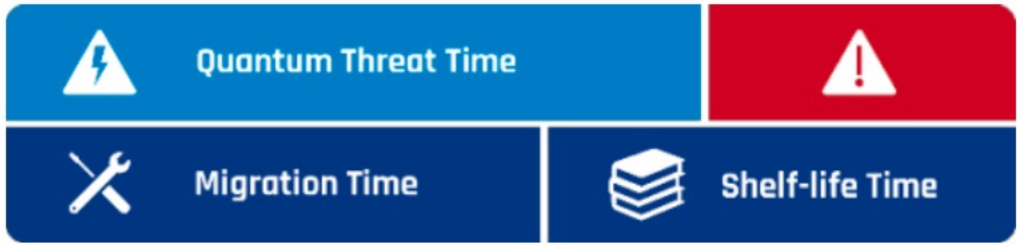
Dr. Michele Mosca

Co-Founder & CEO, evolutionQ Inc.

Dr. Marco Piani

Senior Research Analyst, evolutionQ Inc.

The urgency of moving to quantum-safe cryptography varies for each organization, based on its security needs and risk tolerance.



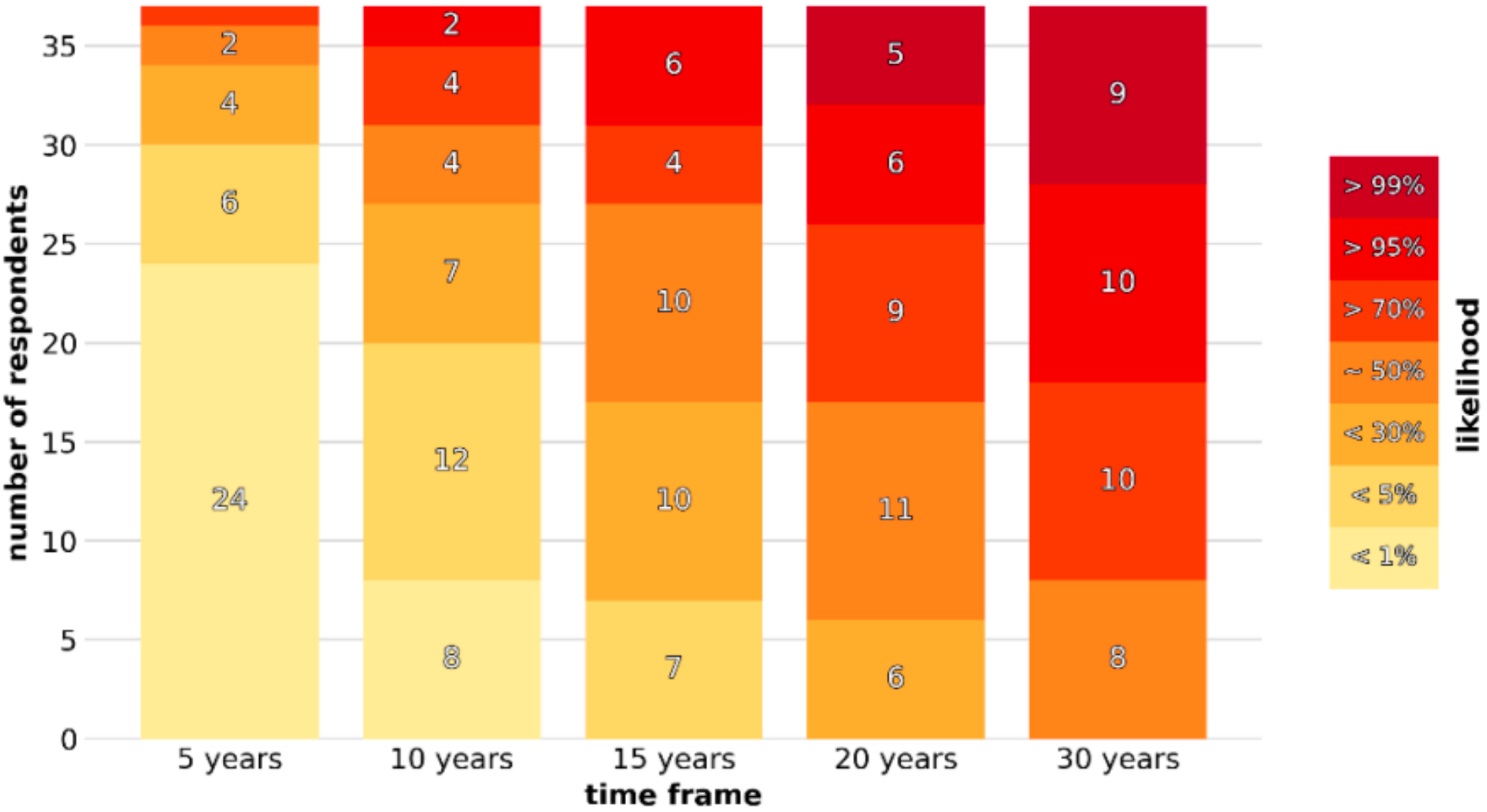
Quantum Threat Time

Migration Time

Shelf-life Time

2023 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

Number of experts who indicated a certain likelihood in each indicated timeframe



Quantum Communication Infrastructure

Report of the DOE
Quantum Internet
Blueprint Workshop

From Long-distance Entanglement to
Building a Nationwide Quantum Internet

February 5-6, 2020

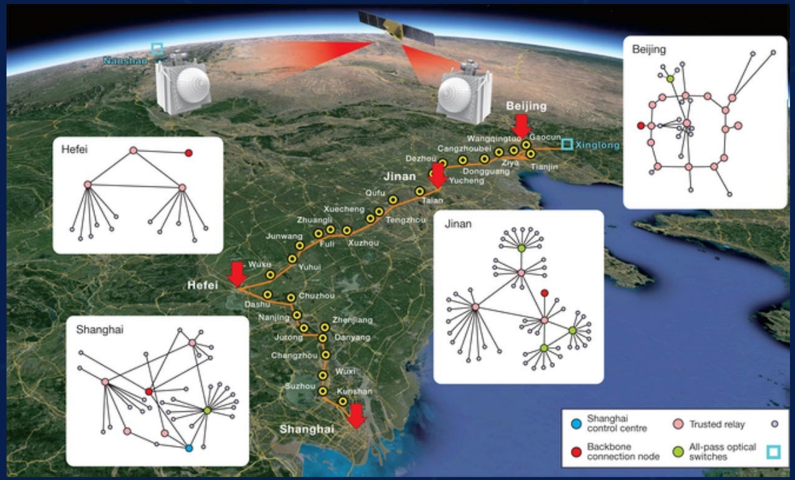
USA

Blueprint for a

quantum internet

European Union

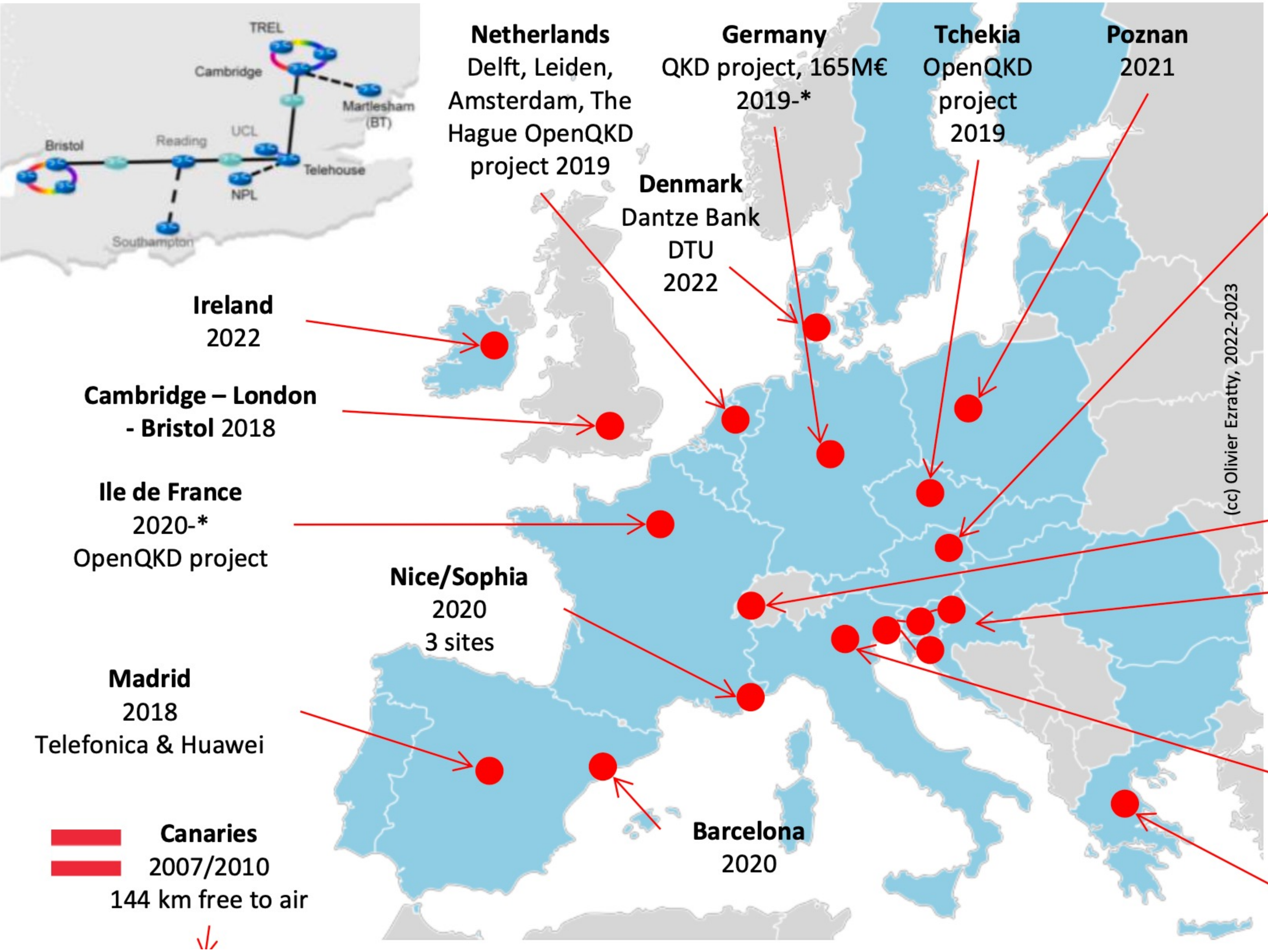
EuroQCI Project



China

3000km distance

Satellite connection



Netherlands
Delft, Leiden, Amsterdam, The Hague OpenQKD project 2019

Germany
QKD project, 165M€
2019-*

Tchekia
OpenQKD project
2019

Poznan
2021

Denmark
Dantze Bank
DTU
2022

Ireland
2022

Cambridge – London - Bristol 2018

Ile de France
2020-*
OpenQKD project

Nice/Sophia
2020
3 sites

Madrid
2018
Telefonica & Huawei

Barcelona
2020

Canaries
2007/2010
144 km free to air

EuroQCI

OPEN QKD

Vienna
2008
SECOQC, 5 nodes, 20/25 km

Geneva
1993, 1995, 2007, 2018 (400 km)

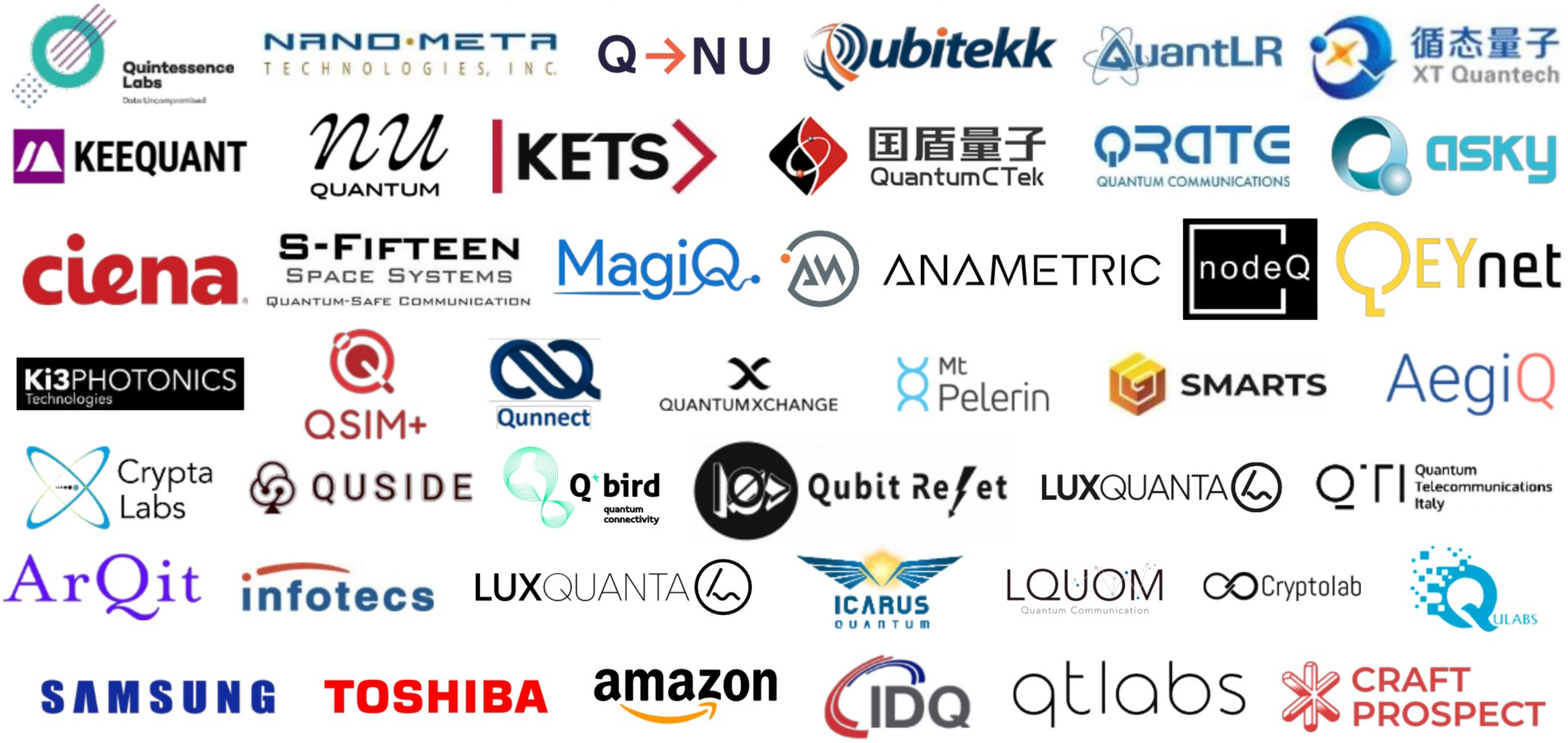
Italy-Slovenia-Croatia network

Italian Quantum Backbone (IQB) 1,850 km QKD link connects Turin, Milan, Bologna, …, a 150 km fiber reaches Modane in France, and connects to Grenoble, Lyon and Paris, then Europe + Padua satellite/ground QKD experiment

Athens
2019
OpenQKD project DataCom

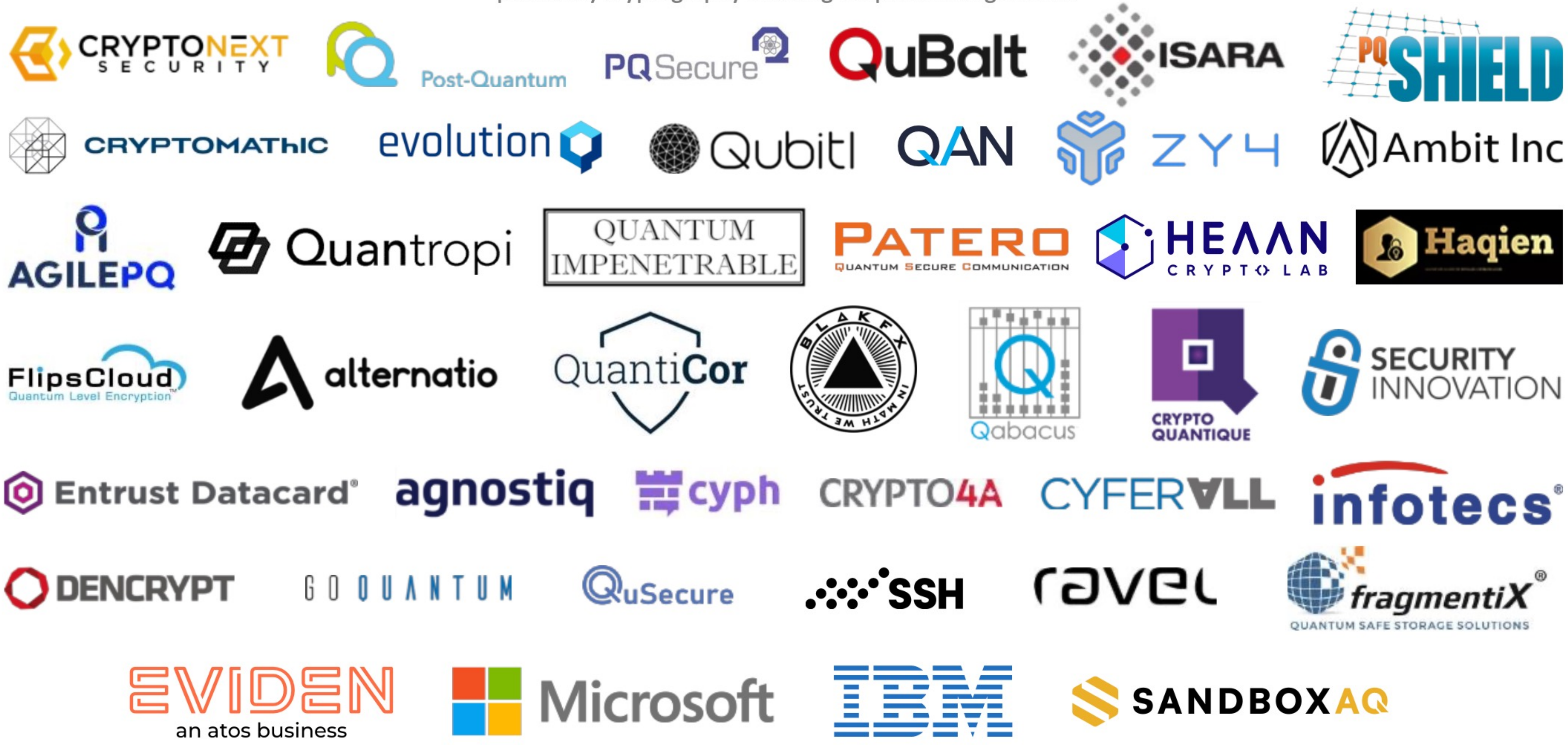
quantum keys QKD / BB84

protects symmetric keys with optical link (fiber or sat)

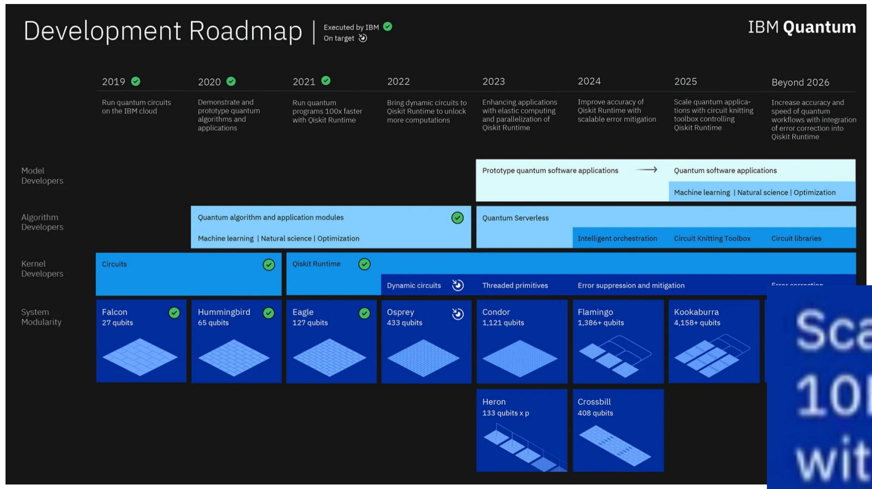


post-quantum cryptography

public key cryptography resisting to quantum algorithms



Privacy = Integrity = Scalability = Quantum Link



Development Roadmap | Executed by IBM ✓ On target

IBM Quantum

2019 ✓ Run quantum circuits on the IBM cloud

2020 ✓ Demonstrate and prototype quantum algorithms and applications

2021 ✓ Run quantum programs 100x faster with Qiskit Runtime

2022 Bring dynamic circuits to Qiskit Runtime to unlock more computations

2023 Enhancing applications with elastic computing and parallelization of Qiskit Runtime

2024 Improve accuracy of Qiskit Runtime with scalable error mitigation

2025 Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime

Beyond 2026 Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime

Model Developers: Prototype quantum software applications → Quantum software applications; Machine learning | Natural science | Optimization

Algorithm Developers: Quantum algorithm and application modules ✓; Machine learning | Natural science | Optimization; Quantum Serverless; Intelligent orchestration; Circuit Knitting Toolbox; Circuit libraries

Kernel Developers: Circuits ✓; Qiskit Runtime ✓; Dynamic circuits; Threaded primitives; Error suppression and mitigation; Error correction

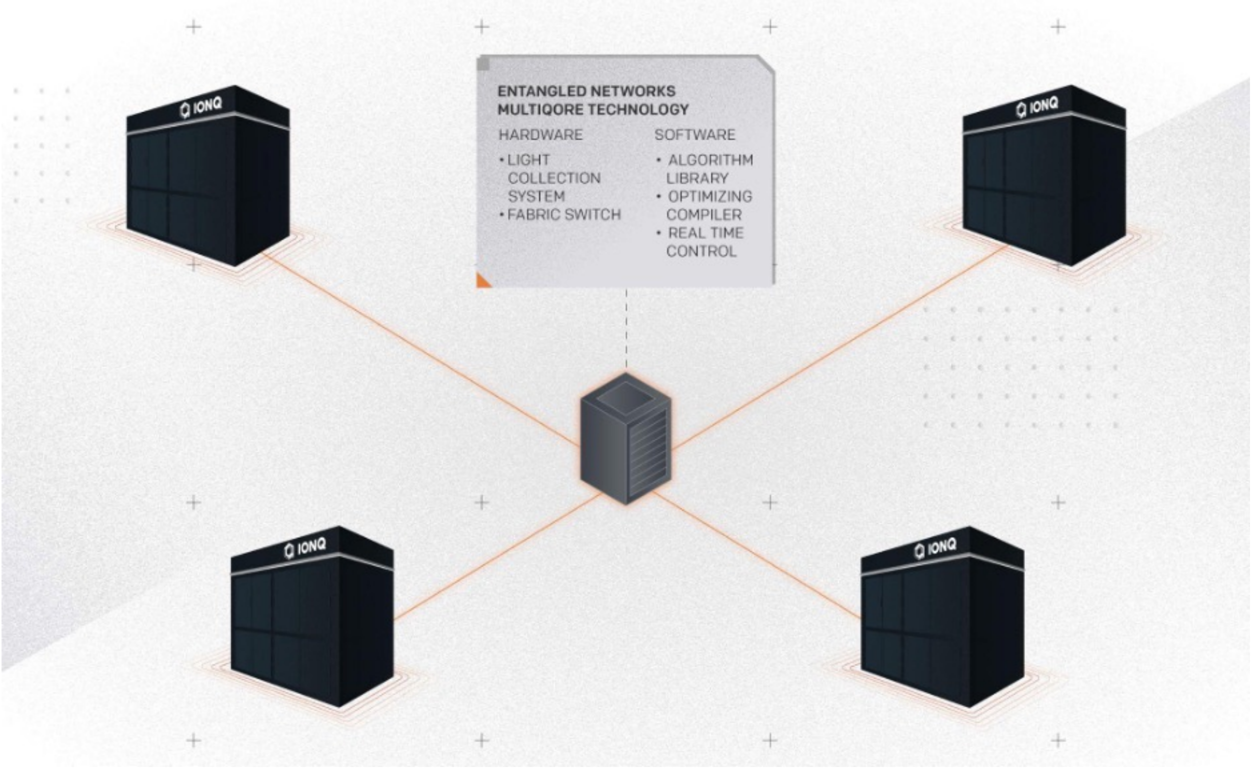
System Modularity: Falcon 27 qubits ✓; Hummingbird 65 qubits ✓; Eagle 127 qubits ✓; Osprey 433 qubits; Condor 1,121 qubits; Flamingo 1,386+ qubits; Kookaburra 4,158+ qubits; Heron 133 qubits x p; Crossbill 408 qubits

Scaling to 10K-100K qubits with classical and quantum communication

nu QUANTUM

QPHOX

WeLinQ



ENTANGLED NETWORKS
MULTIQORE TECHNOLOGY

HARDWARE
- LIGHT COLLECTION SYSTEM
- FABRIC SWITCH

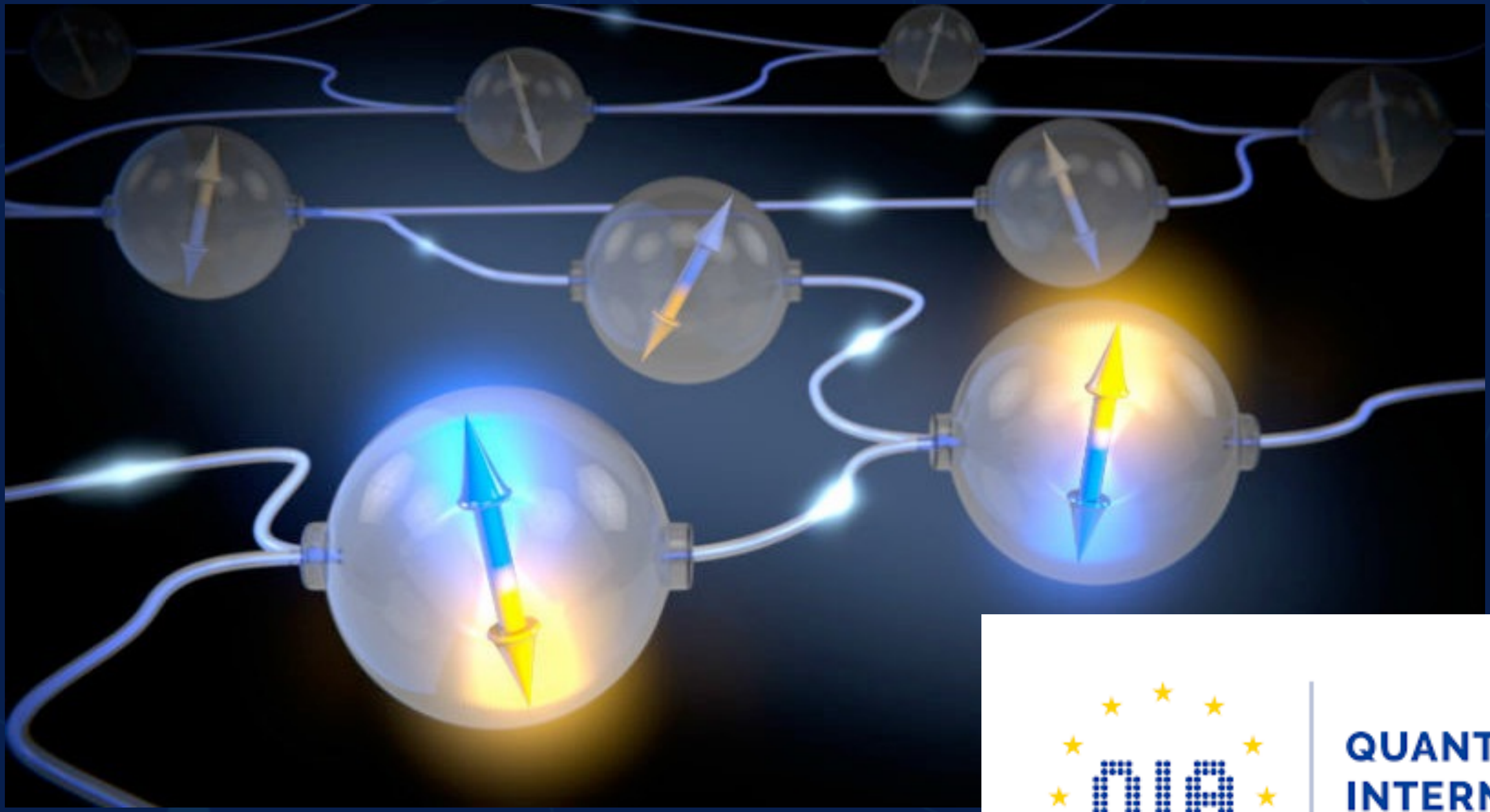
SOFTWARE
- ALGORITHM LIBRARY
- OPTIMIZING COMPILER
- REAL TIME CONTROL

IONQ

Entangled Networks

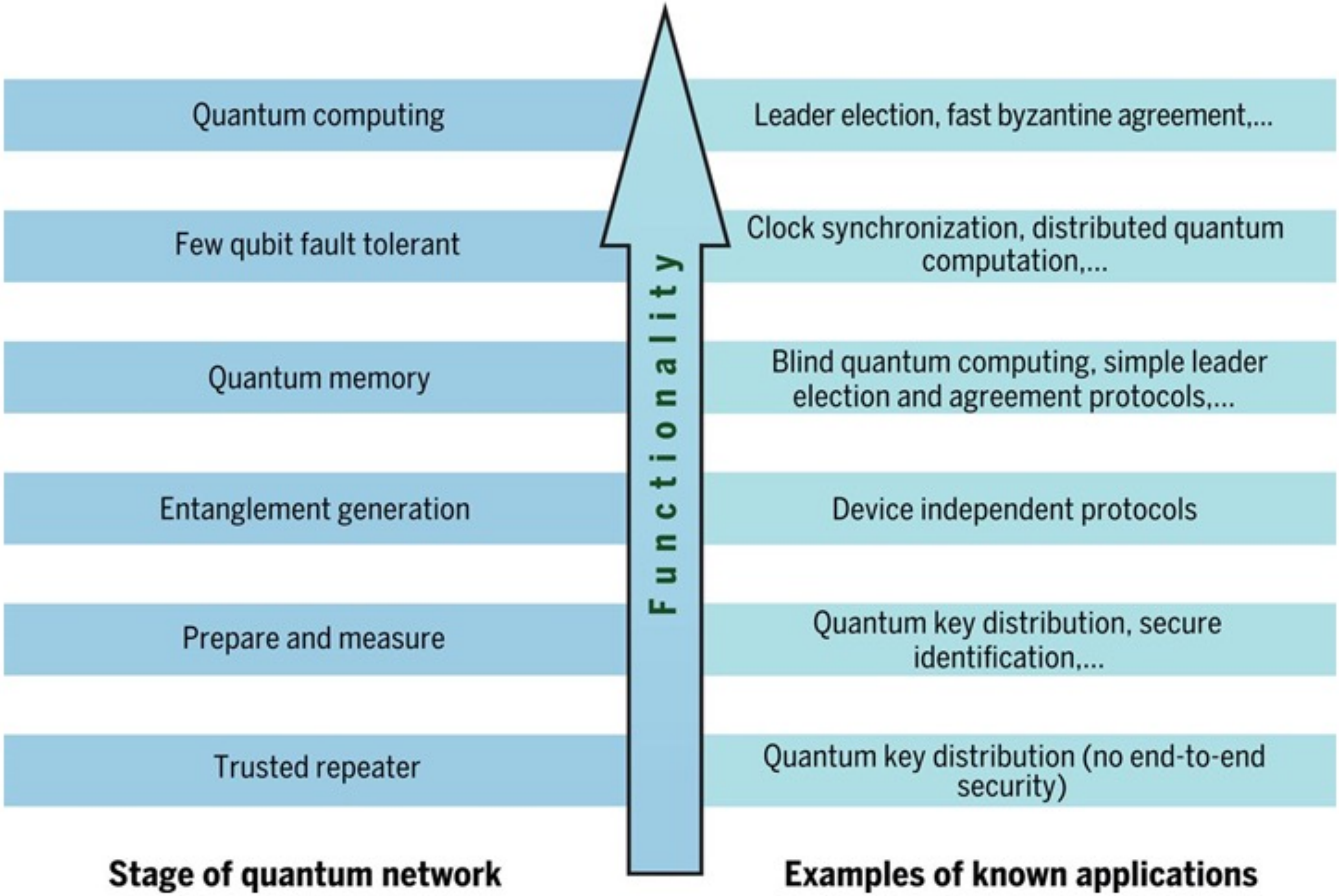
Quantum Internet

Quantum Computer + Quantum Communication



QUANTUM INTERNET ALLIANCE

Quantum network stages



Functionality

Stage of quantum network	Examples of known applications
Quantum computing	Leader election, fast byzantine agreement,...
Few qubit fault tolerant	Clock synchronization, distributed quantum computation,...
Quantum memory	Blind quantum computing, simple leader election and agreement protocols,...
Entanglement generation	Device independent protocols
Prepare and measure	Quantum key distribution, secure identification,...
Trusted repeater	Quantum key distribution (no end-to-end security)

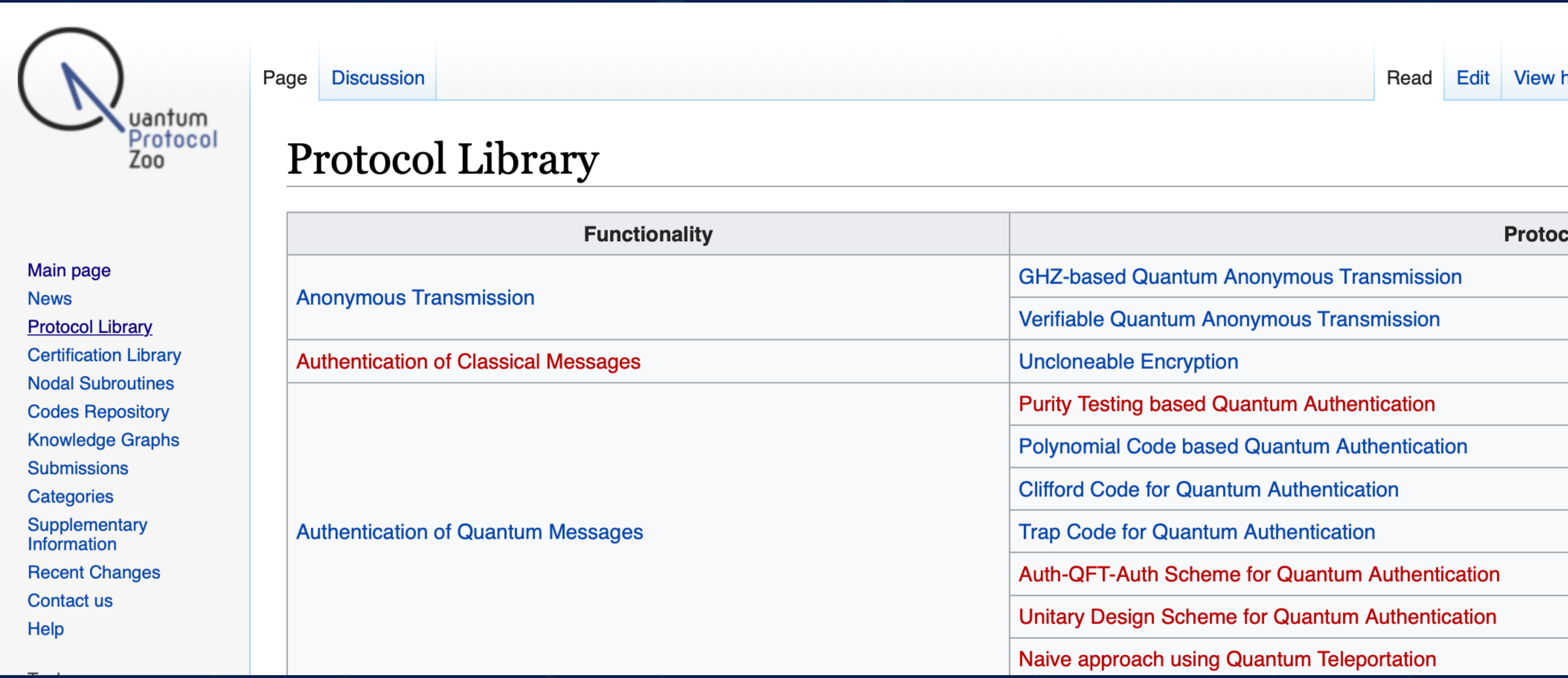
Quantum internet: A vision for the road ahead, Stephanie Wehner, David Elkouss, Ronald Hanson Science 2018

The Quantum Protocol Zoo

Shraddha Singh,[1] Mina Doosti,[2] Natansh Mathur,[1, 3] Rhea Parekh,[1, 4] Gözde Ustün,[1] Bas Dirkse,[5, 6, 7]
Victoria Lipinska,[5, 6] Jérémy Ribeiro,[5, 6] Mahshid Delavar,[2] Niraj Kumar,[2] Gláucia Murta,[5, 6]
Atul Mantri,[2] Celine Chevalier,[8] Harold Ollivier,[1] Marc Kaplan,[9] and Elham Kashefi[1, 2, *]

Quantum Protocol Zoo

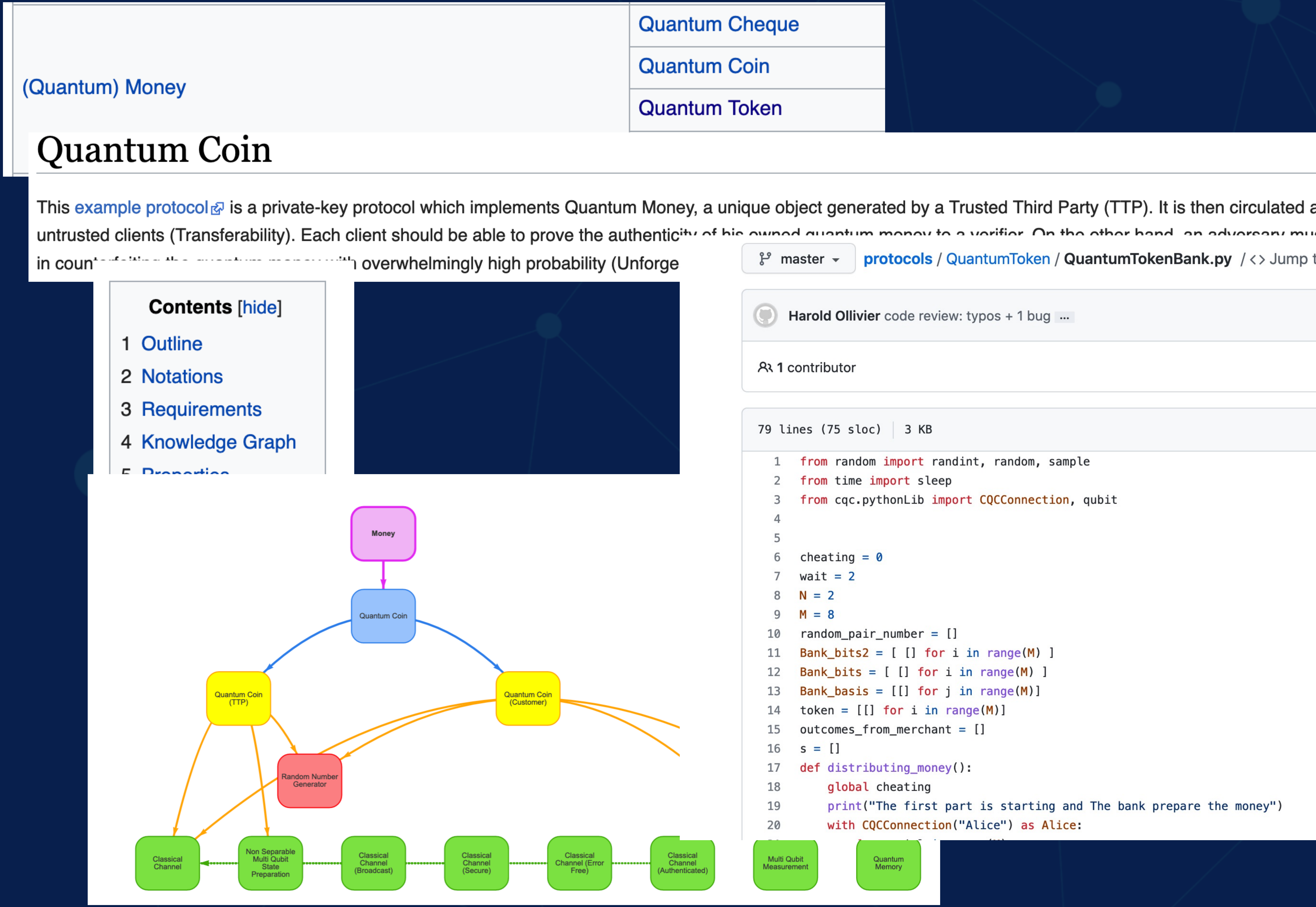
https://wiki.veriqloud.fr/



- Main page
- News
- Protocol Library
- Certification Library
- Nodal Subroutines
- Codes Repository
- Knowledge Graphs
- Submissions
- Categories
- Supplementary Information
- Recent Changes
- Contact us
- Help

Protocol Library

Functionality	Protoc
Anonymous Transmission	GHZ-based Quantum Anonymous Transmission
	Verifiable Quantum Anonymous Transmission
Authentication of Classical Messages	Uncloneable Encryption
Authentication of Quantum Messages	Purity Testing based Quantum Authentication
	Polynomial Code based Quantum Authentication
	Clifford Code for Quantum Authentication
	Trap Code for Quantum Authentication
	Auth-QFT-Auth Scheme for Quantum Authentication
	Unitary Design Scheme for Quantum Authentication
	Naive approach using Quantum Teleportation



(Quantum) Money

Quantum Cheque

Quantum Coin

Quantum Token

Quantum Coin

This example protocol is a private-key protocol which implements Quantum Money, a unique object generated by a Trusted Third Party (TTP). It is then circulated a untrusted clients (Transferability). Each client should be able to prove the authenticit of his owned quantum money to a verifier. On the other hand, an adversary mu in coun overwhelmingly high probability (Unforge

Money
Quantum Coin
Quantum Coin (TTP)
Quantum Coin (Customer)
Random Number Generator
Classical Channel
Non Separable Multi Qubit State Preparation
Classical Channel (Broadcast)
Classical Channel (Secure)
Classical Channel (Error Free)
Classical Channel (Authenticated)
Multi Qubit Measurement
Quantum Memory

master / protocols / QuantumToken / QuantumTokenBank.py / <> Jump t

Harold Ollivier code review: typos + 1 bug ...

1 contributor

79 lines (75 sloc) | 3 KB

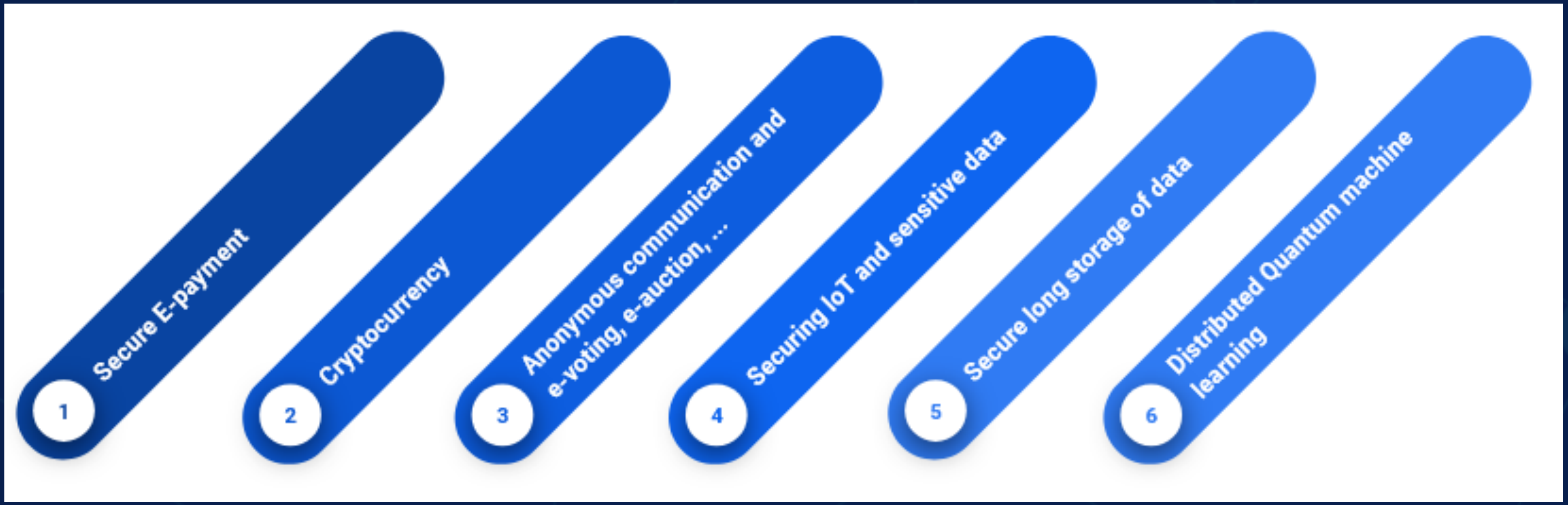
```
from random import randint, random, sample
from time import sleep
from cqc.pythonLib import CQCConnection, qubit


cheating = 0
wait = 2
N = 2
M = 8
random_pair_number = []
Bank_bits2 = [ [] for i in range(M) ]
Bank_bits = [ [] for i in range(M) ]
Bank_basis = [[] for j in range(M)]
token = [[] for i in range(M)]
outcomes_from_merchant = []
s = []
def distributing_money():
    global cheating
    print("The first part is starting and The bank prepare the money")
    with CQCConnection("Alice") as Alice:
```

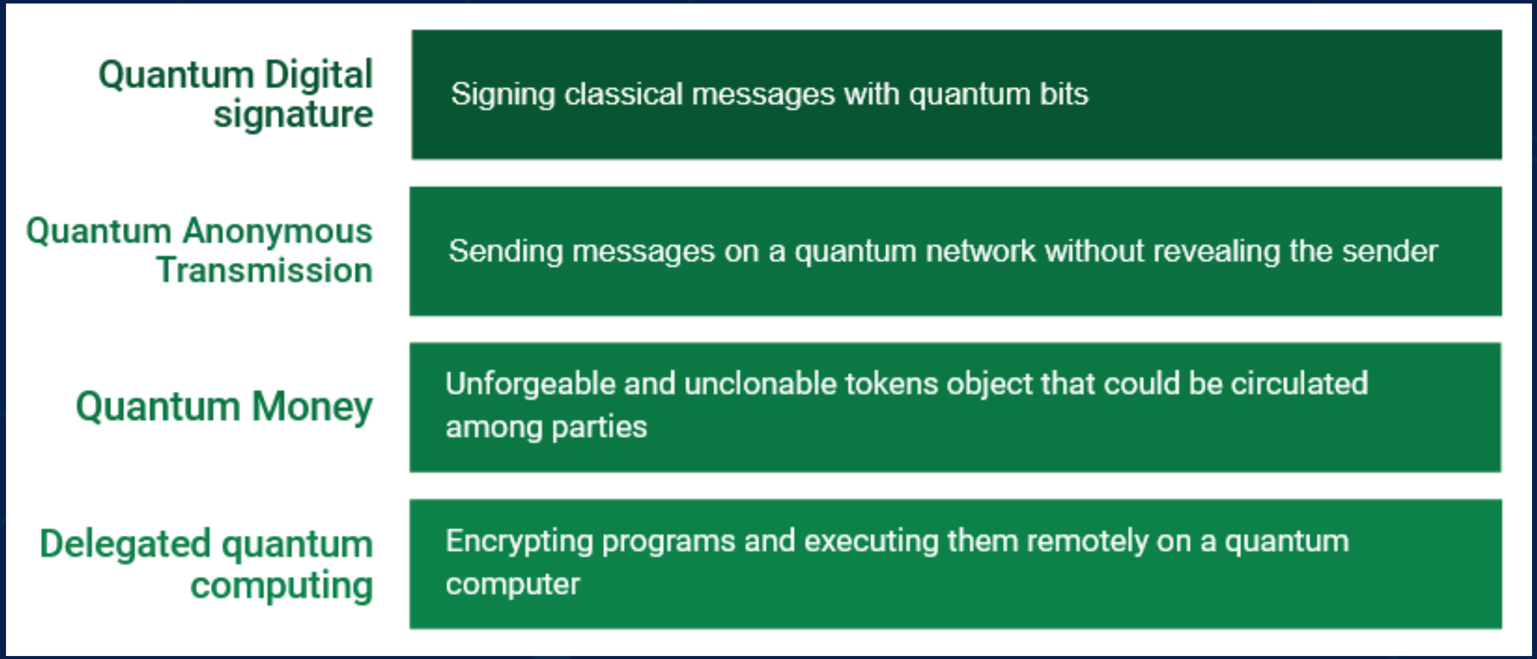
Use-case for future Quantum Internet

QUANTUM INTERNET ALLIANCE

QUANTUM FLAGSHIP



1. Secure E-payment
2. Cryptocurrency
3. Anonymous communication and e-voting, e-auction, ...
4. Securing IoT and sensitive data
5. Secure long storage of data
6. Distributed Quantum machine learning



Quantum Digital signature	Signing classical messages with quantum bits
Quantum Anonymous Transmission	Sending messages on a quantum network without revealing the sender
Quantum Money	Unforgeable and unclonable tokens object that could be circulated among parties
Delegated quantum computing	Encrypting programs and executing them remotely on a quantum computer

Use-case for future Quantum Internet

QUANTUM INTERNET ALLIANCE

QUANTUM FLAGSHIP

Challenge: New Threat models on authentication

Solution: Design an authentication system using unclonable quantum tokens

Challenge: Aggregation of sensitive data from mistrustful parties

Solution: Make privacy by-design long-term secure with the help of quantum resources

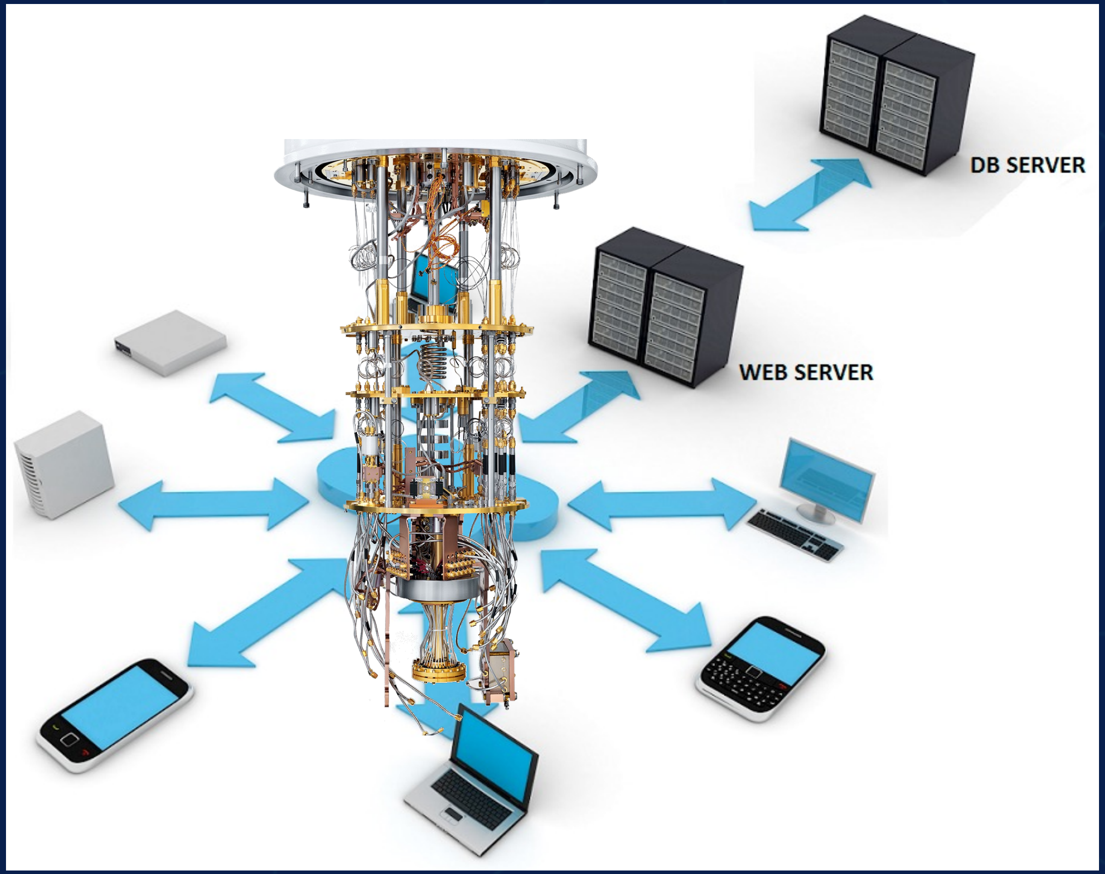
Challenge: Cross-platform finance

Solution: Design a Quantum SWIFT system
secure cross-chain operations using unforgeable quantum tokens

Challenge: Data Privacy with Quantum Machine learning

Solution: Use the noise of quantum networks to make QML private by-design

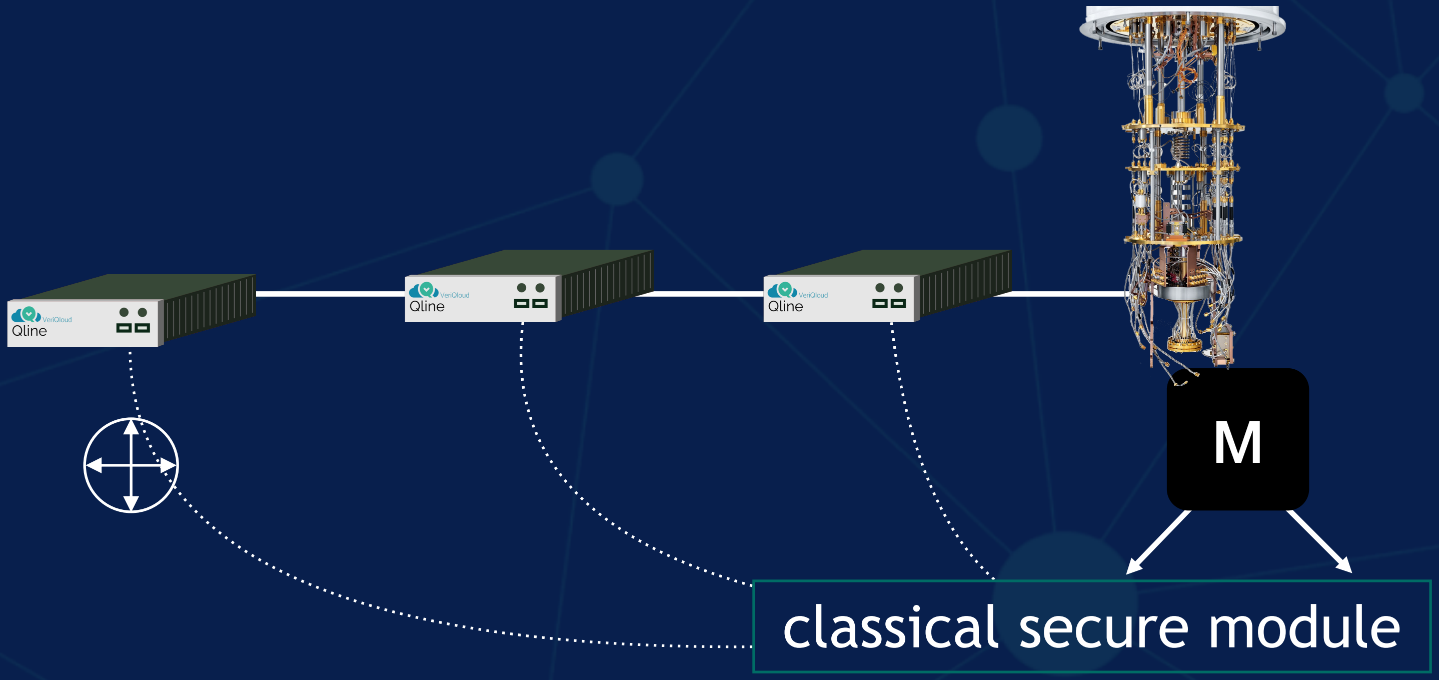
Current Pain Point Quantum Cloud Provider



No privacy - No verifiability

Data, Algorithms, Outcomes are all knowns to hardware provider

Quantum-safe quantum cloud infrastructure



classical secure module

Qline: clients' data encryption

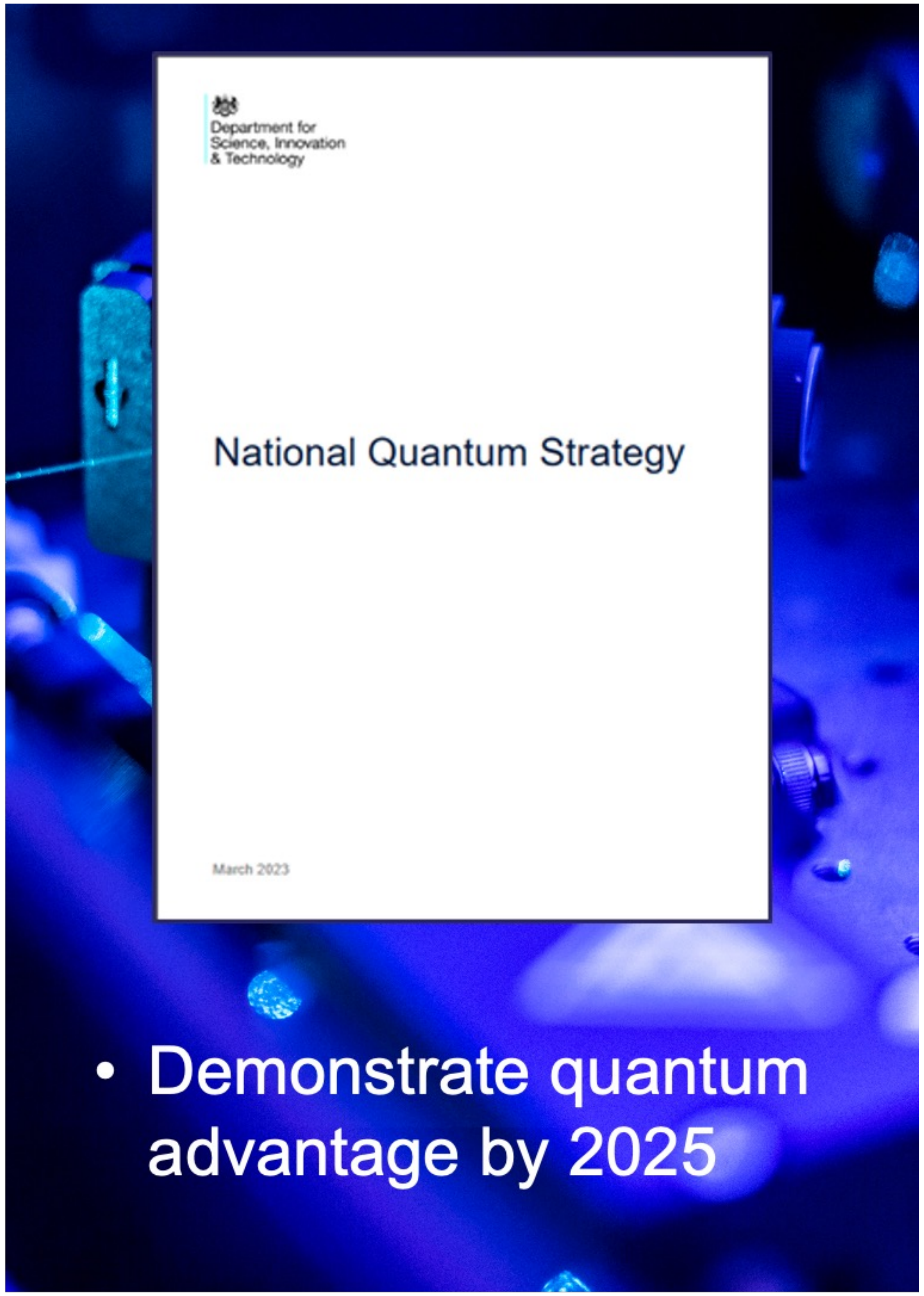
Gate teleportation: computing on encrypted quantum data

Quantum Computing Mission

The mission seeks to drive the development of test-beds and applications to underpin further growth of a UK quantum computing sector capable of delivering quantum advantage in 2025

The funding is supporting a number of delivery strands:

- **Up to £30 m** for the **Quantum Computing Testbed Development** call – **competition launched 21 Aug, closes 4 Oct**
- **£6 m Software-Enabled Quantum Computation** call with EPSRC – **launched 12 Dec 2022, closed 1 February 2023**
- **£8 m Feasibility Studies in Quantum Computing Applications** call with Innovate UK – **launched 13 Feb 2023, closed 29 March 2023**
- **£6 m** investments directly through the NQCC:
  - **Innovation Hub** at Harwell Campus
  - **User engagement programme, SparQ**, and quantum readiness training
  - **Quantum computing as a service (QCaaS)**



Department for
Science, Innovation
& Technology

National Quantum Strategy

March 2023

- Demonstrate quantum advantage by 2025

Policy paper

National Quantum Strategy Missions

Updated 14 December 2023

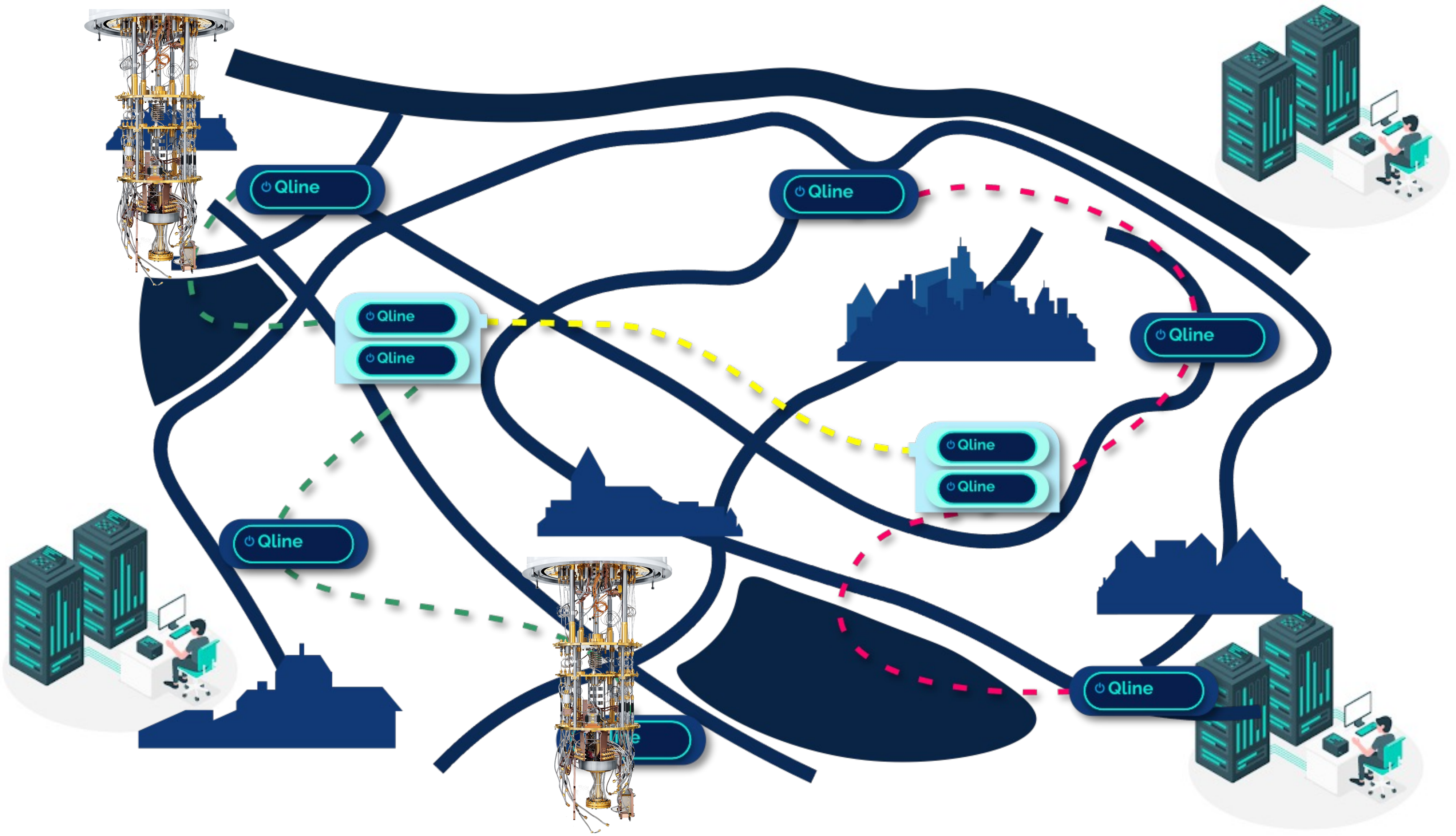
- **Mission 1**
- By 2035, there will be accessible, UK-based quantum computers capable of running 1 trillion operations and supporting applications that provide benefits well in excess of classical supercomputers across key sectors of the economy.
- **Mission 2**
- By 2035, the UK will have deployed the world's most advanced quantum network at scale, pioneering the future quantum internet.
- **Mission 3**
- By 2030, every NHS Trust will benefit from quantum sensing- enabled solutions, helping those with chronic illness live healthier, longer lives through early diagnosis and treatment.
- **Mission 4**
- By 2030, quantum navigation systems, including clocks, will be deployed on aircraft, providing next-generation accuracy for resilience that is independent of satellite signals.
- **Mission 5**
- By 2030, mobile, networked quantum sensors will have unlocked new situational awareness capabilities, exploited across critical infrastructure in the transport, telecoms, energy, and defence sectors.

By 2028, extending beyond the NISQ-era with 10 a million quantum operations, which will enable the exploration of applications associated with the simulation of chemical processes, helping to improve catalyst design for example.

By 2032, demonstrating large-scale error correction capabilities with 10 billion quantum operations, with applications including accelerated drug discovery.

By 2035, achieving quantum advantage at scale through reaching 10 a trillion quantum operations, enabling applications such as optimising the production of clean hydrogen.

Quantum Utopia: Secure Quantum Data Center


Qline
Qline
Qline
Qline
Qline
Qline
Qline
Qline
Qline