Quantum Advantage Pathfinder

Elham Kashefi

University of Edinburgh
National Quantum Computing Center
CNRS Sorbonne University

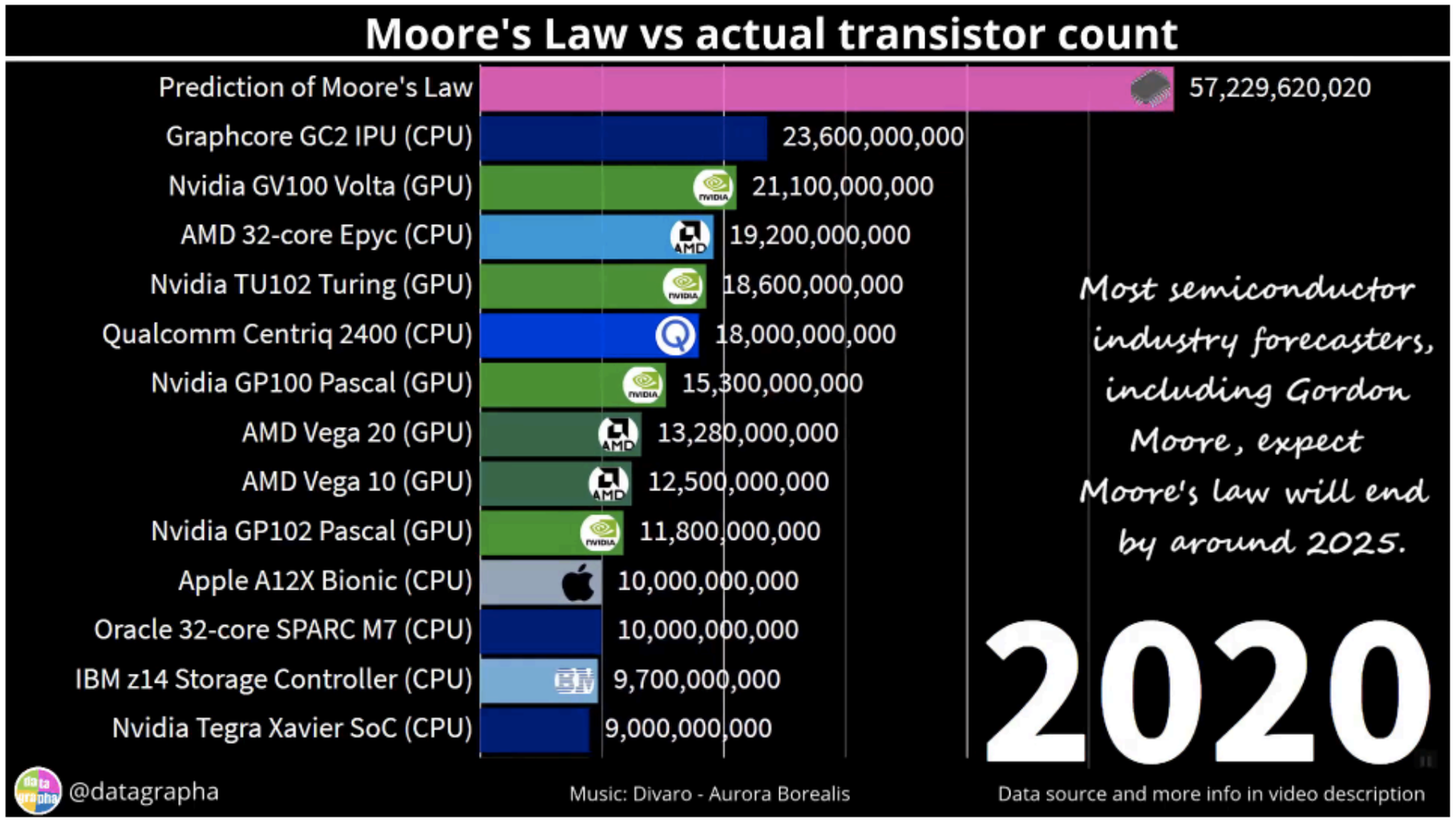
Big Data Machine

Collection/Correlation/Communication/Trading

Big Data Machine

Collection/Correlation/Communication/Trading

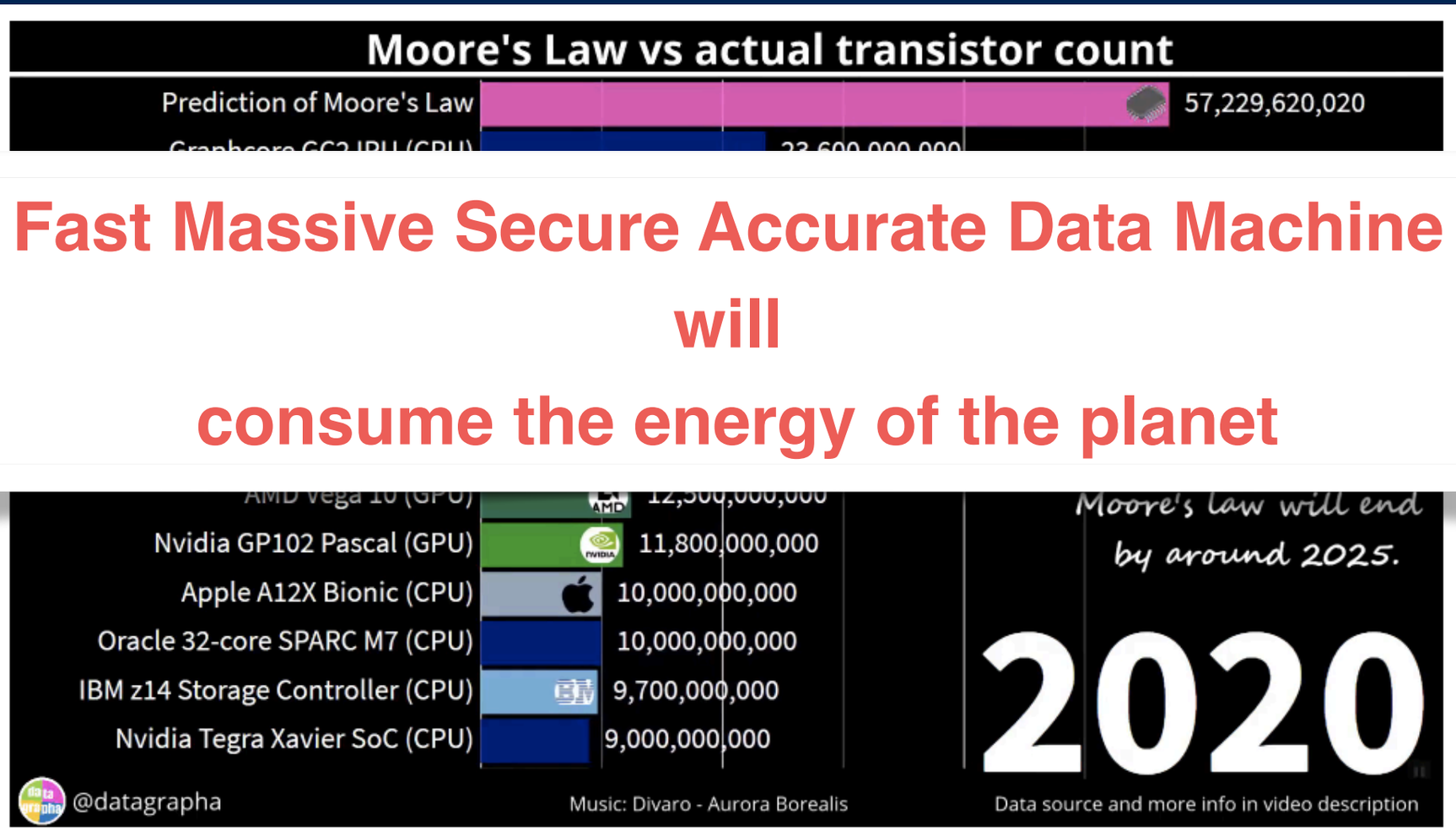
Computing Machine



Big Data Machine

Collection/Correlation/Communication/Trading

Computing Machine

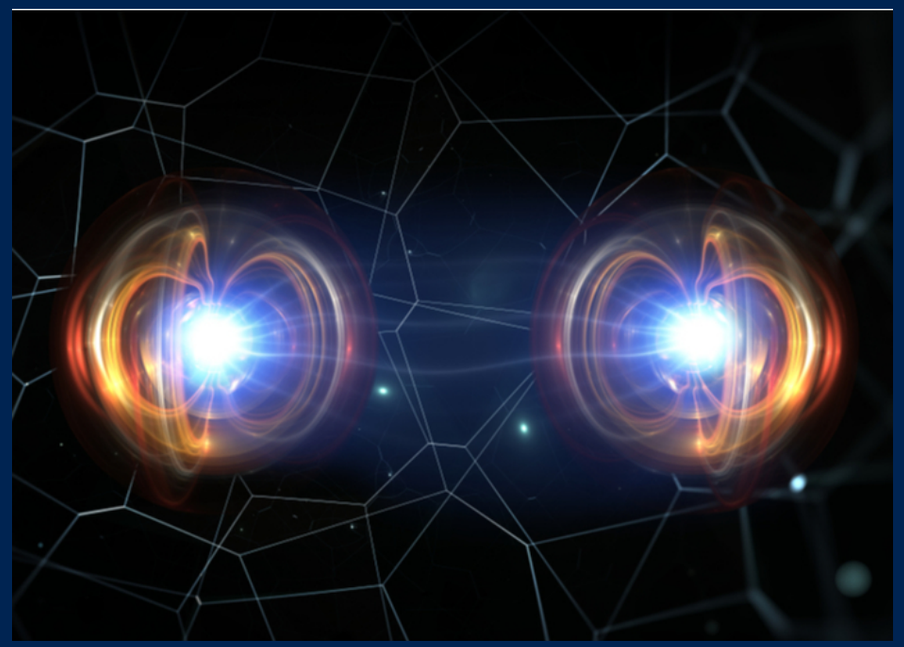


Fast Massive Secure Accurate Data Machine
will
consume the energy of the planet

Breaking the Barrier

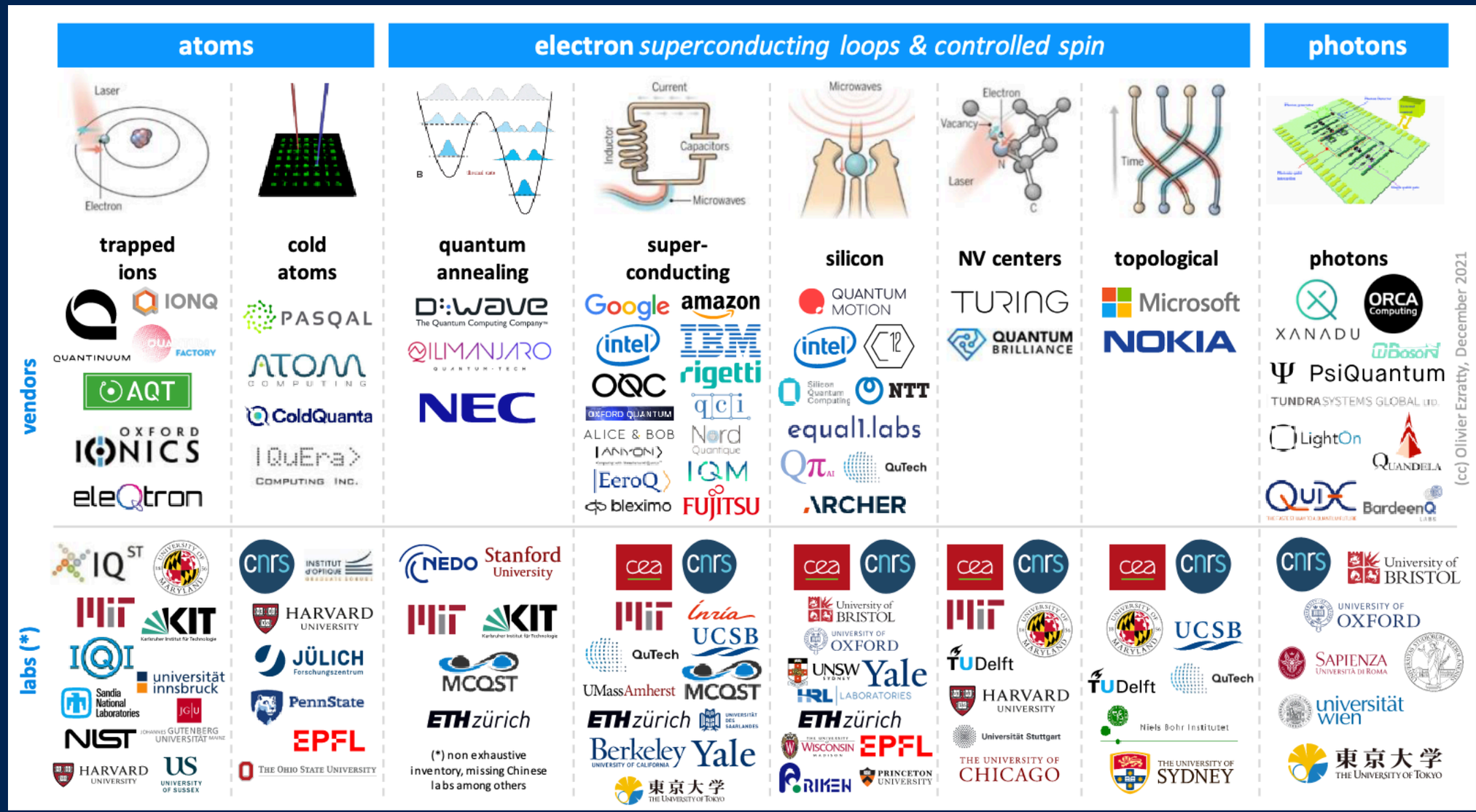
Breaking the Barrier

either 0 or 1
measurement reveals the value
can be copied
bits string of are described locally

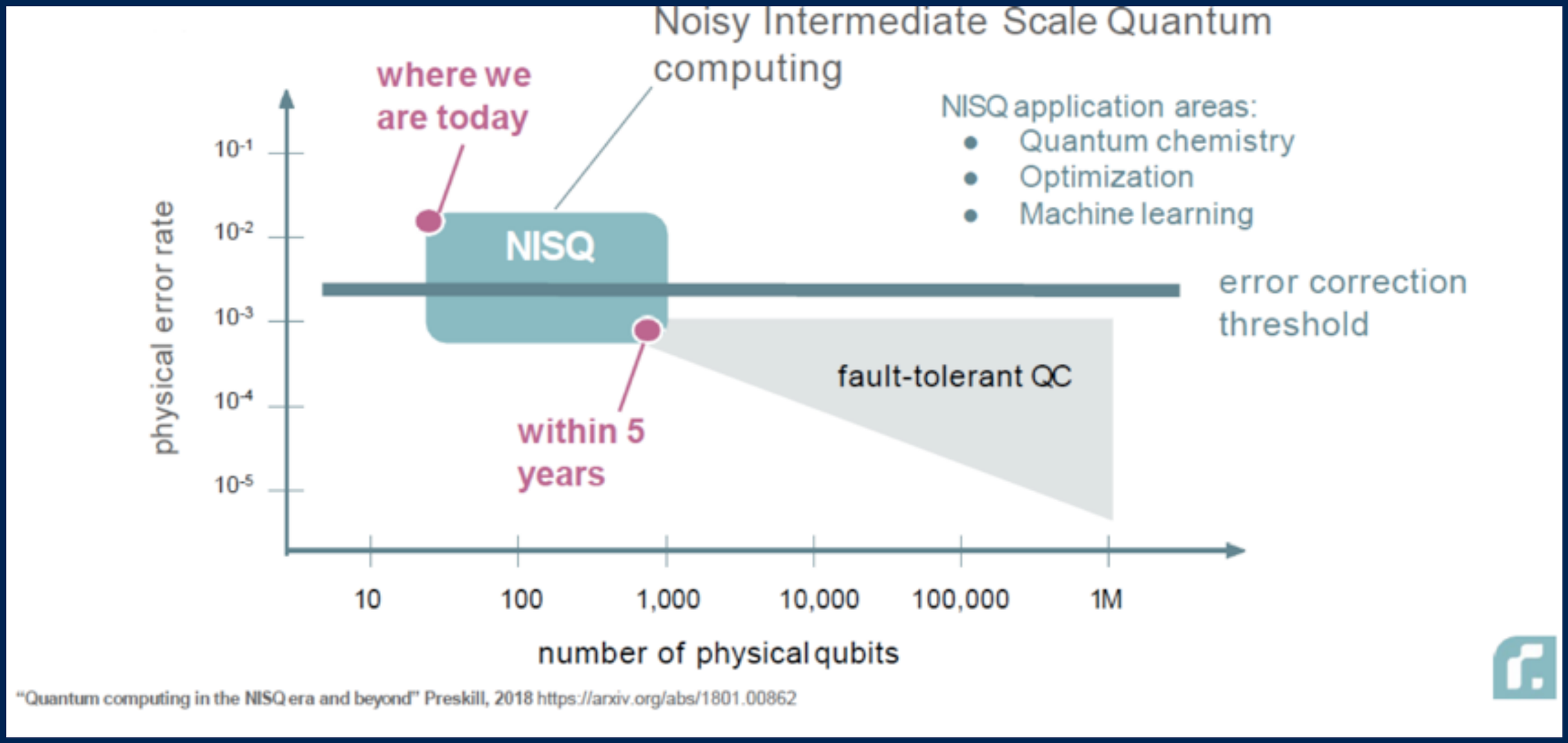


simultaneously 0 and 1
measurement changes the value
cannot be copied
qubits string exhibit non-local correlations

Speed = Quantum Hardware



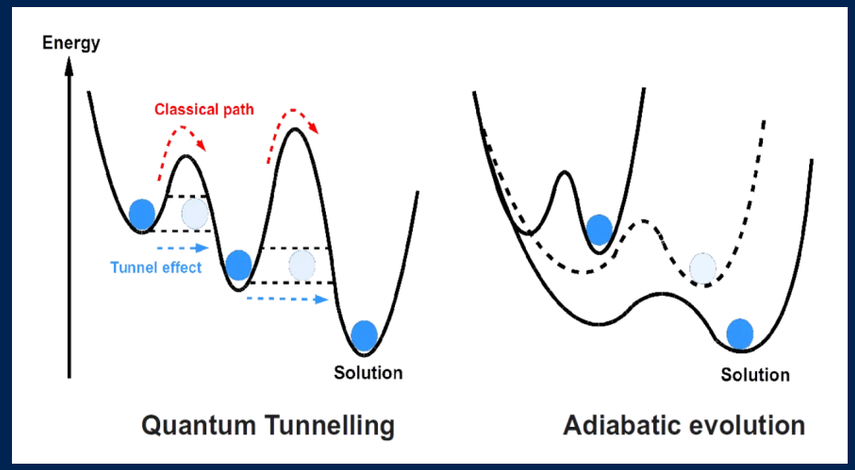
Speed = Quantum Hardware



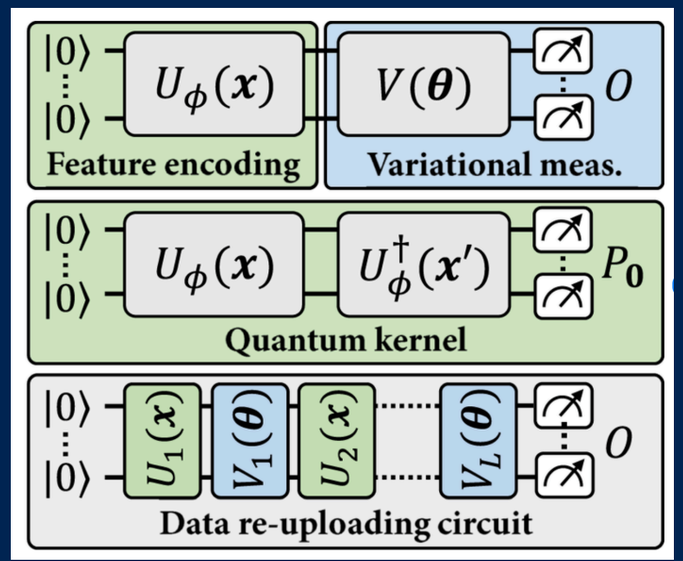
"Quantum computing in the NISQ era and beyond" Preskill, 2018 https://arxiv.org/abs/1801.00862

Speed = Quantum Hardware

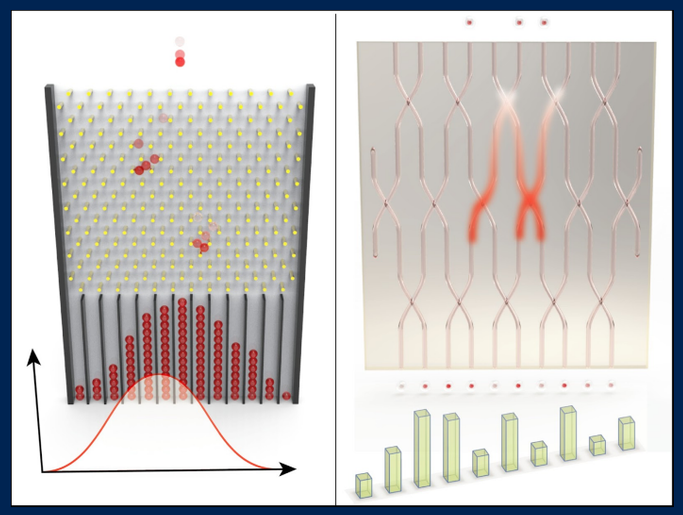
Optimisation → Quantum Annealing



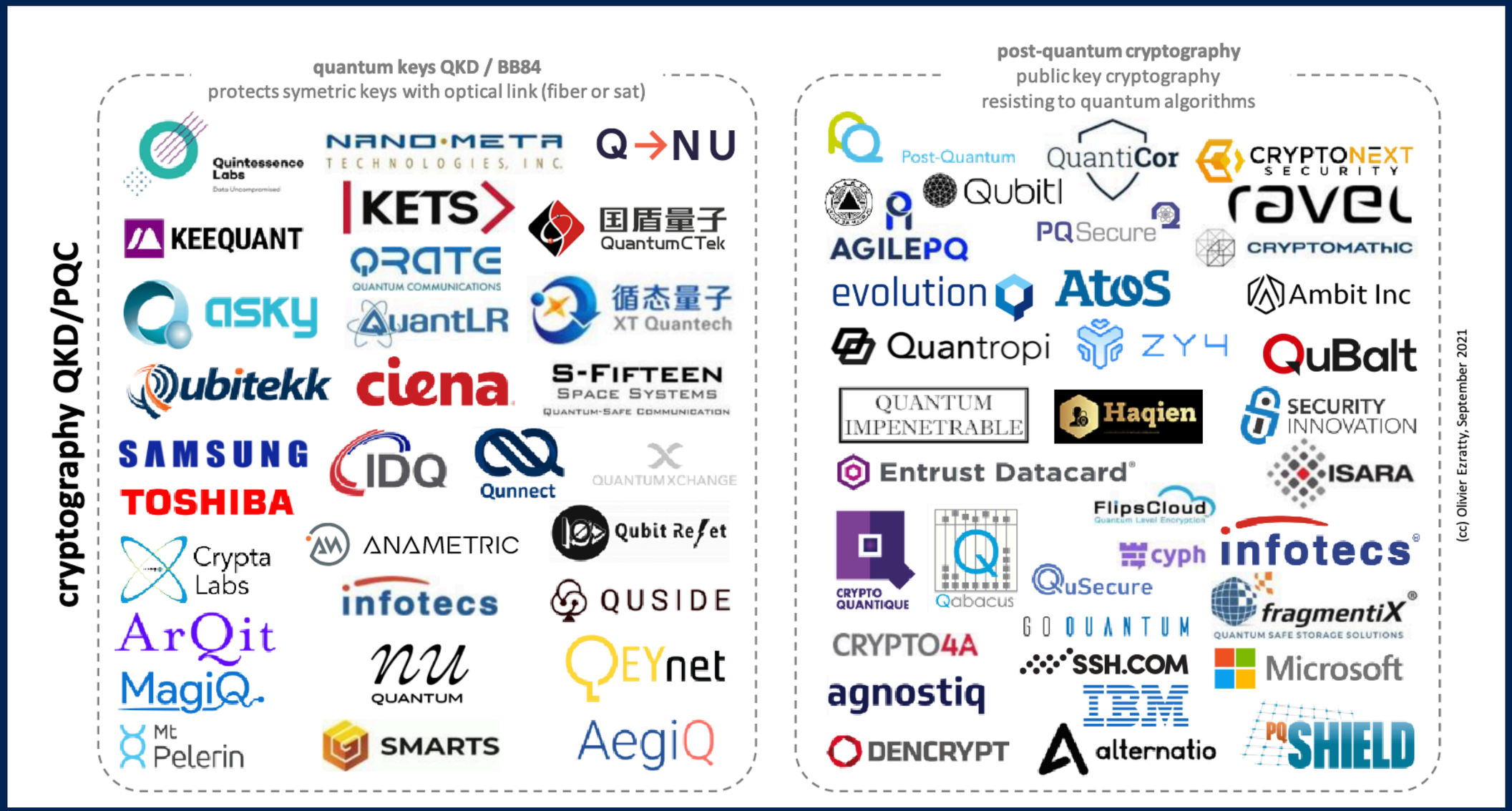
Linear Algebra → Quantum ML



Monte Carlo Simulation → Quantum Sampling



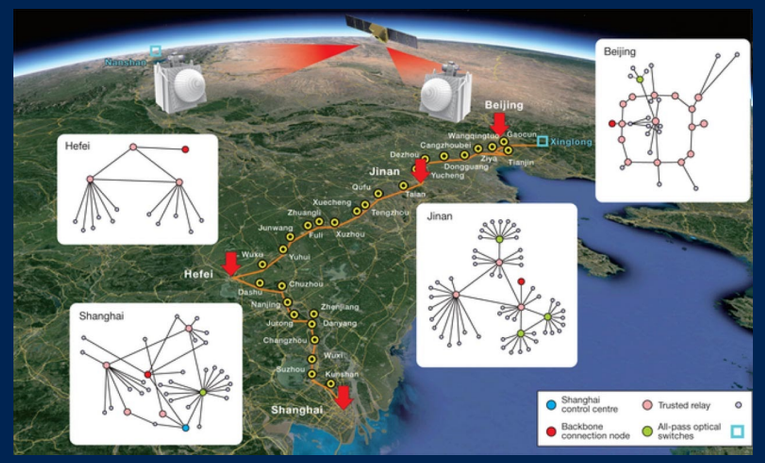
Security = Quantum Communication



Security = Quantum Communication

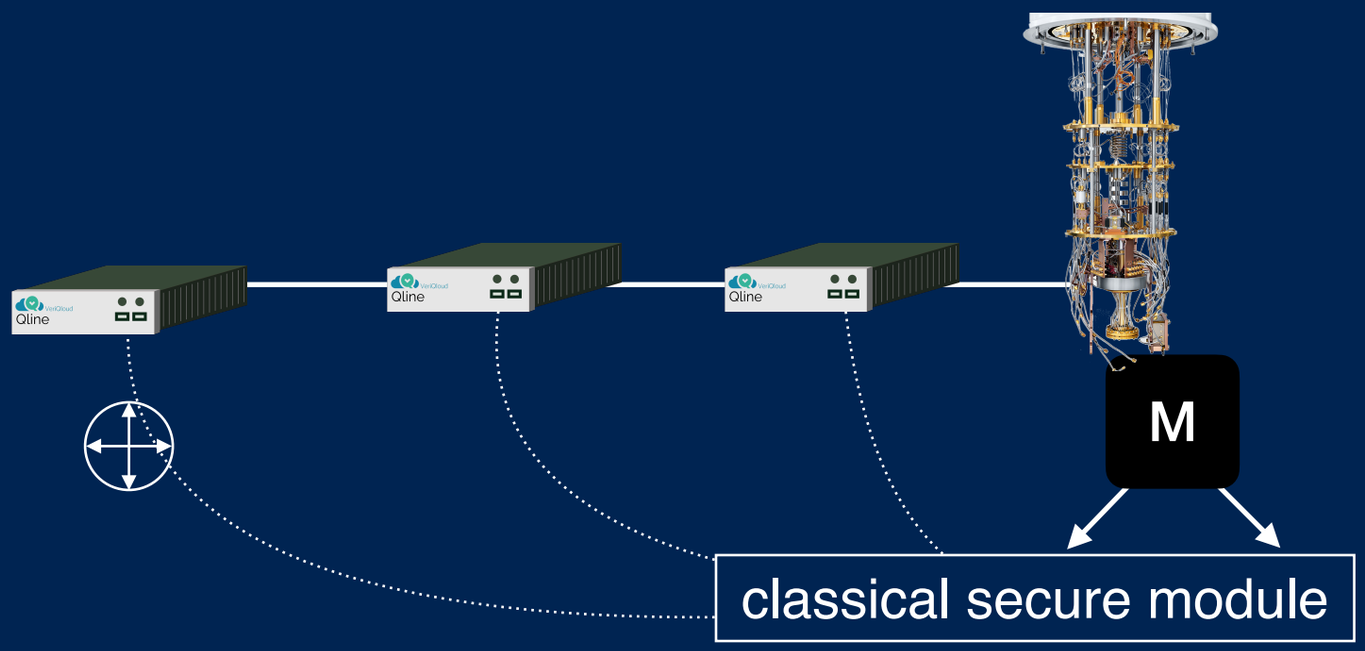
USA
Blueprint for a quantum internet

European Union
EuroQCI Project



China
3000km distance
Satellite connection

Security + Speed = Quantum Internet



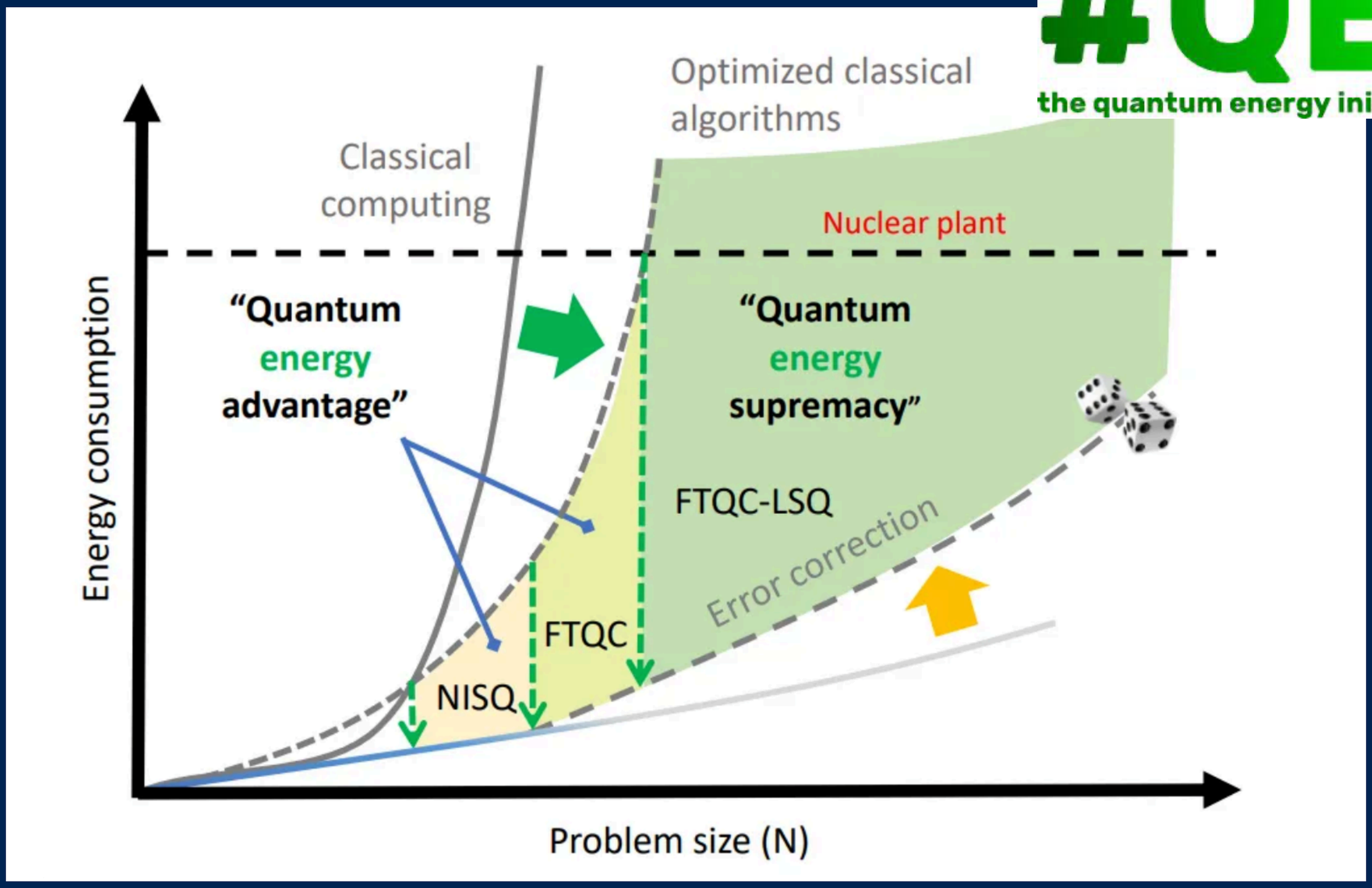
Random Qubit: clients data encryption

Gate teleportation: computing on encrypted quantum data

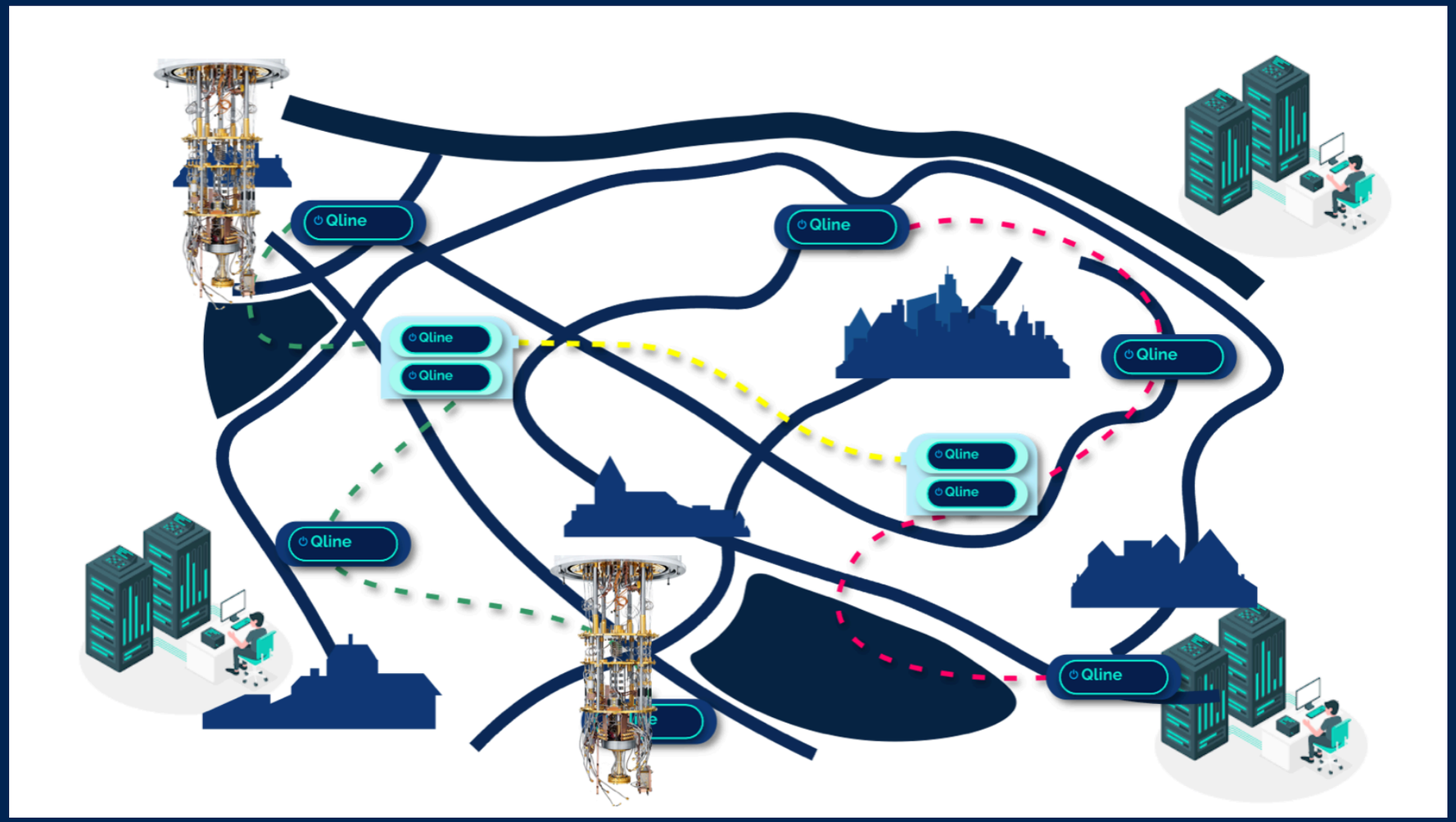
Trapification: publicly verifiable outsource computing

Energy Efficiency

#QEI
the quantum energy initiative



Future Secure Fast Quantum Data Machine For Public Good



Net Zero - Health - Fraud detection
Regulated Computing - Privacy Preserving

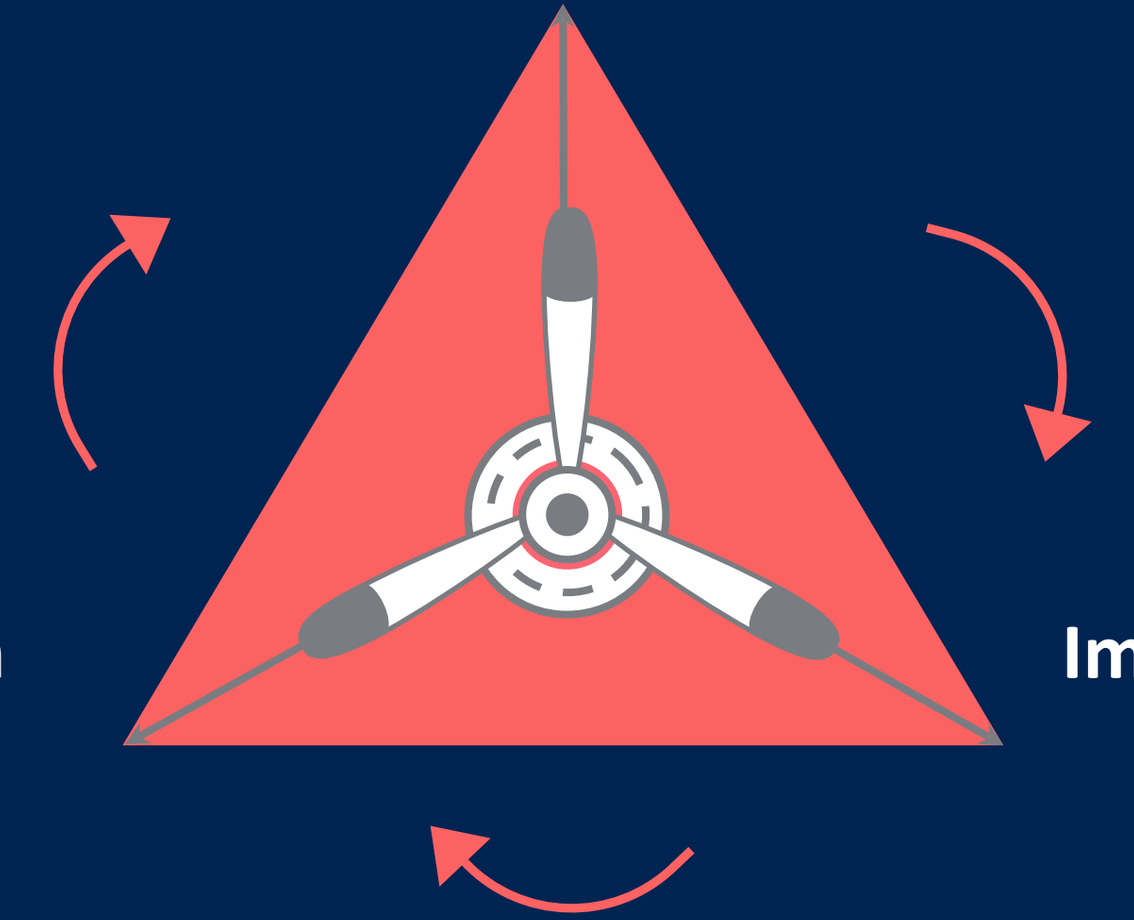
Quantum Utopia

Quantum Utopia

It takes an *ecosystem* to raise a *useful* quantum application

Quantum Software Lab

Discovery
Science



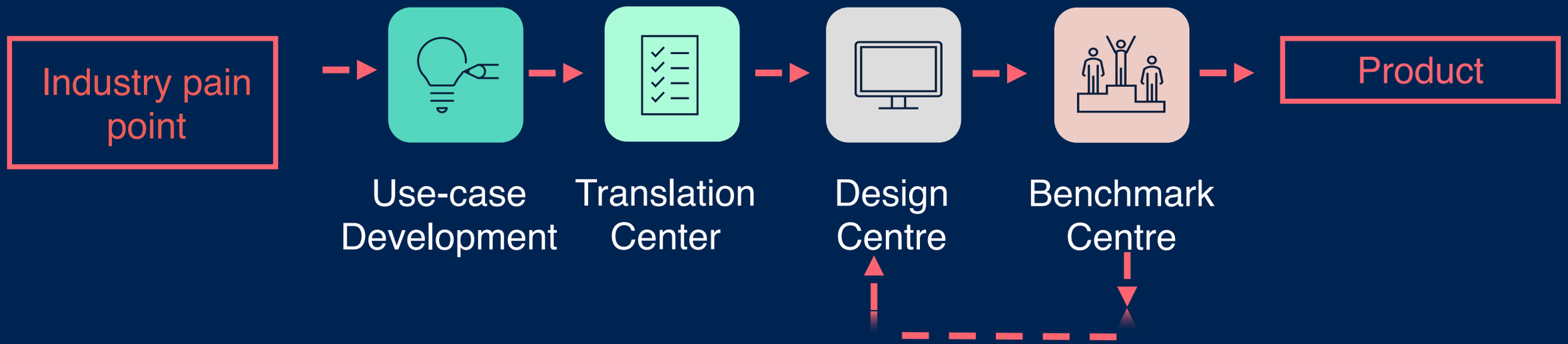
Exploitation
Use case

Implementation
Technology

Quantum Software Lab

60+ researchers **400+ papers** **30+ projects**

Start up culture inside an academic institute



Quantum Software Lab

Universiteit Leiden

IQC Institute for Quantum Computing

Joint Center for Quantum Information and Computer Science

Inria

Quantum Computing & Simulation Hub

Quantum Computing Application Cluster

QIA Quantum Internet Alliance

Sorbonne Université

Sydney Quantum Academy

東京大学 The University of Tokyo

VeriQloud

Quandela

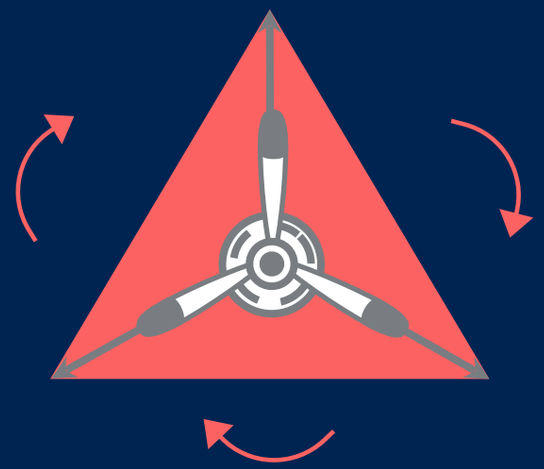
PASQAL

IONQ

OQC

aws

QPARC



Cisco

UKRI Innovate UK

CQC Cambridge Quantum Computing

river lane

ORCA Computing

nu Quantum

rigetti

UKRI National Quantum Computing Centre

epcc

UKRI Science and Technology Facilities Council

Hartree Centre

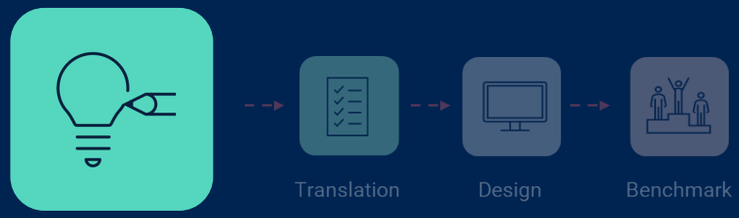
The Alan Turing Institute

NPL National Physical Laboratory

Following our Scottish route to perform the best quantum show

*"... showcase new scripts, especially ones on more obscure, edgy, or unusual material. The lack of ~~artistic~~ **VC** vetting combined with free entry make risk-taking more feasible."*

The Edinburgh Festival fringe
Defying the norm since 1947



Use-case Development

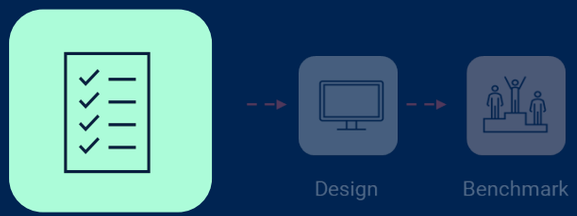
Engage industry experts and practitioners through targeted outreach and collaboration

Conduct in-depth **surveys** to identify industry pain points and unmet needs

Reverse Pitch Challenge event to gather direct industry input and feedback, with continued involvement of industry experts to help define the identified use cases

Quantum Computing & Simulation Hub

AIM DAY



Translation Centre

which parts of use-case may benefit from which quantum support ?

Top-down:

Requirements analysis

Translate industry figure of merit into properties of mathematical model to be developed

Bottom-up:

Develop mathematical abstractions

Known problem templates with specific requirements using particular quantum resources

epcc | Inria | lfcs Laboratory for Foundations of Computer Science

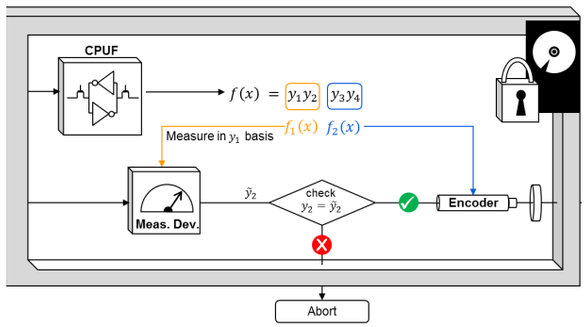
Design Centre

Benchmark

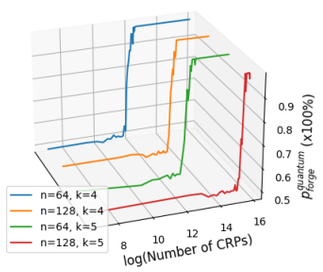
TEMPLATES

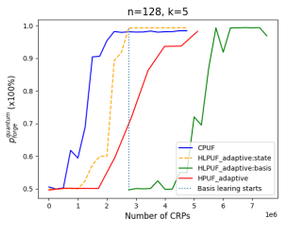
PROPERTIES

Systematisation of Knowledge / Optimisation / Design of Quantum Algorithms



Simulations





Formal Analysis / Complexity Analysis

The game $\mathcal{G}^{\mathcal{F}}_{q,c,\mu}(\lambda,\mathcal{A})$[a]

Setup phase:

- $\texttt{param} \leftarrow \mathcal{S}(\lambda)$
- The oracles $\mathcal{O}^{\mathcal{E}}$ and $\mathcal{O}^{\mathcal{V}}$ and the message space $\mathcal{M}$ are instantiated given $\texttt{param}$.

Selective challenge phase:

- if $c = \mathsf{qSel}$: $\mathcal{A}$ picks $m \in \mathcal{M}$ and sends it to $\mathcal{C}$.

First learning phase:

- $\mathcal{A}$ issues queries $\rho_1^{in}, \ldots, \rho_q^{in}$ (where $q = poly(\lambda)$) to $\mathcal{C}$. To each query ρ_i^{in} the challenger $\mathcal{C}$ queries $\mathcal{O}^{\mathcal{E}}$ on ρ_i^{in}, and forwards the received respective output ρ_i^{out} to $\mathcal{A}$. The adversary can also have an internal register σ which may be entangled with the output queries.

Challenge phase:

- if $c = \mathsf{qEx}$: $\mathcal{A}$ picks $m \in \mathcal{M}$ and sends it to $\mathcal{C}$.
- if $c = \mathsf{qUni}$: $\mathcal{C}$ picks $m \xleftarrow{\$} \mathcal{M}$ uniformly at random and sends m to $\mathcal{A}$

Second learning phase: As the *first learning phase*
Guess phase:

- if $c = \mathsf{qEx}$ OR $c = \mathsf{qSel}$: continue if $m \notin_{\mu} \rho^{in}$.[b]
- $\mathcal{A}$ generates the forgery t, and outputs to $\mathcal{C}$ the pair $(m,t) \leftarrow \mathcal{A}(\{\rho_i^{in}, \rho_i^{out}\}_{i=1}^{q}, \sigma)$
- $\mathcal{C}$ queries the verification oracle: $b \leftarrow \mathcal{O}^{\mathcal{V}}(m,t)$
- $\mathcal{C}$ outputs b

[a] $c \in \{\mathsf{qEx}, \mathsf{qSel}, \mathsf{qUni}\}$; $0 < \mu \leq 1$.
[b] $\notin_{\mu} \rho^{in}$ denotes at least μ-distinguishability from all the ρ_i^{in}. For the classical message $m \in \{0,1\}^n$, the condition should hold for $|m\rangle$, i.e. the quantum encoding of m in computational basis.

nu QUANTUM

QUANTUM COMPUTING APPLICATION CLUSTER

Quantum Computing & Simulation Hub

cisco

rigetti

river Lane

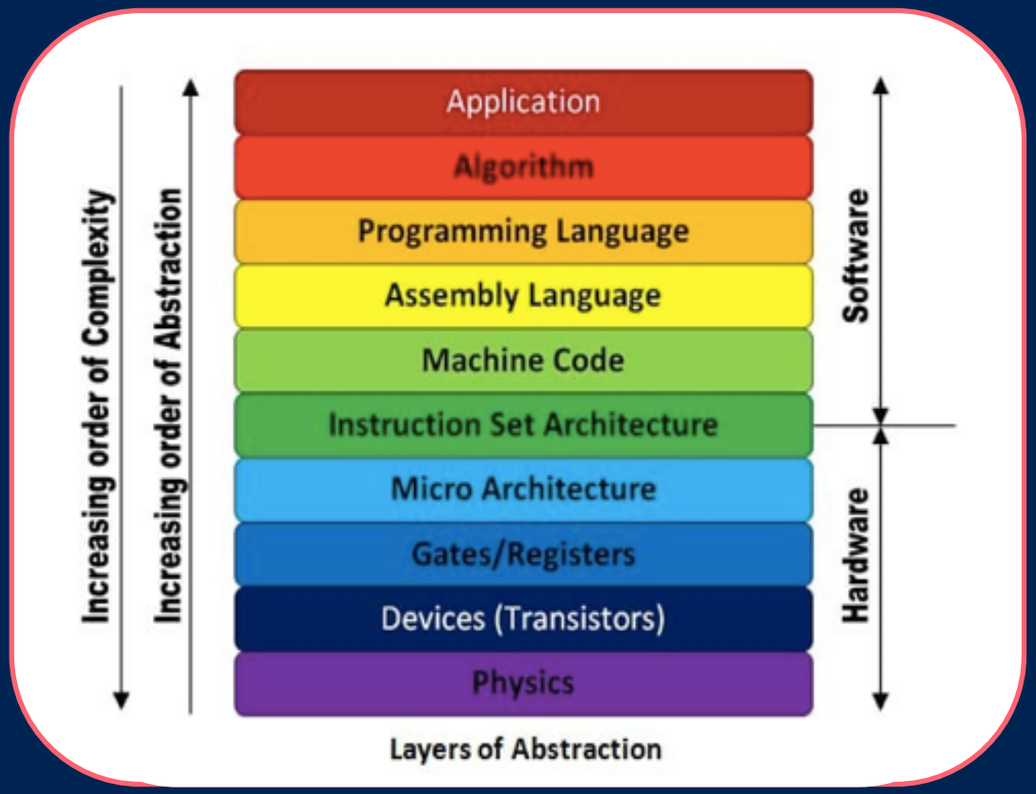
CAMBRIDGE QUANTUM COMPUTING

ORCA Computing

Implementation Centre

Optimal allocation of quantum and classical computing resources

Adapting classical ICT methodology



epcc | icsa Institute for Computing Systems Architecture

Benchmark Centre

Error/noise characterisation and mitigation

Certification of the quality of the solution

End-to-end feasibility report for each use case

Comparison / benchmarking with best possible classical

Benchmarking of hardware and of the implementation

Verification of the computation

Benchmark Centre

Quantum Advantage

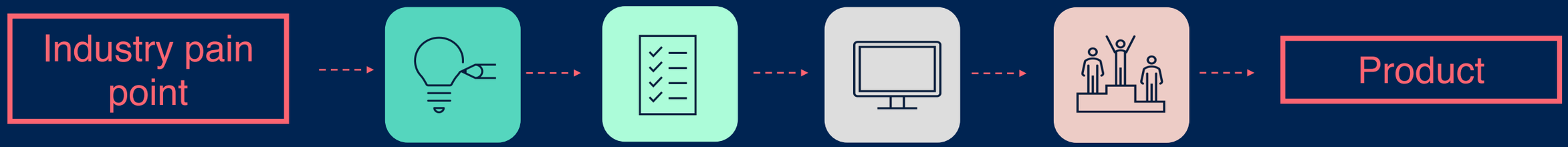
Can be achieved now, and with which platform

How it can be achieved in the future

Why it cannot be achieved

Quantum Synthetic Data - a case study

Differential Privacy
Quantum Machine
Learning



Privacy &
Accuracy

Standard Chartered

LIP6

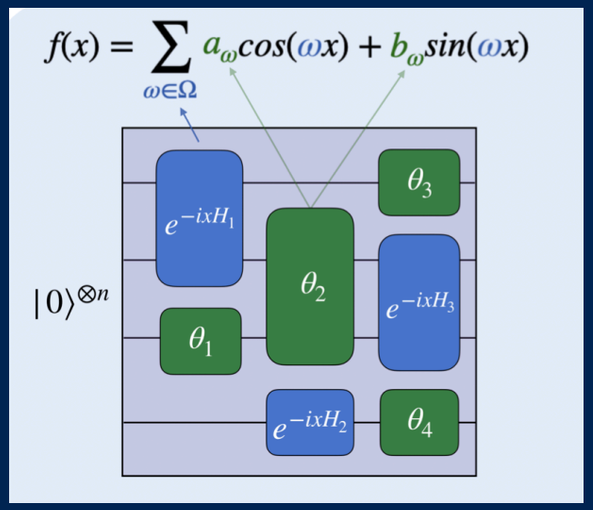
VeriQloud

rigetti

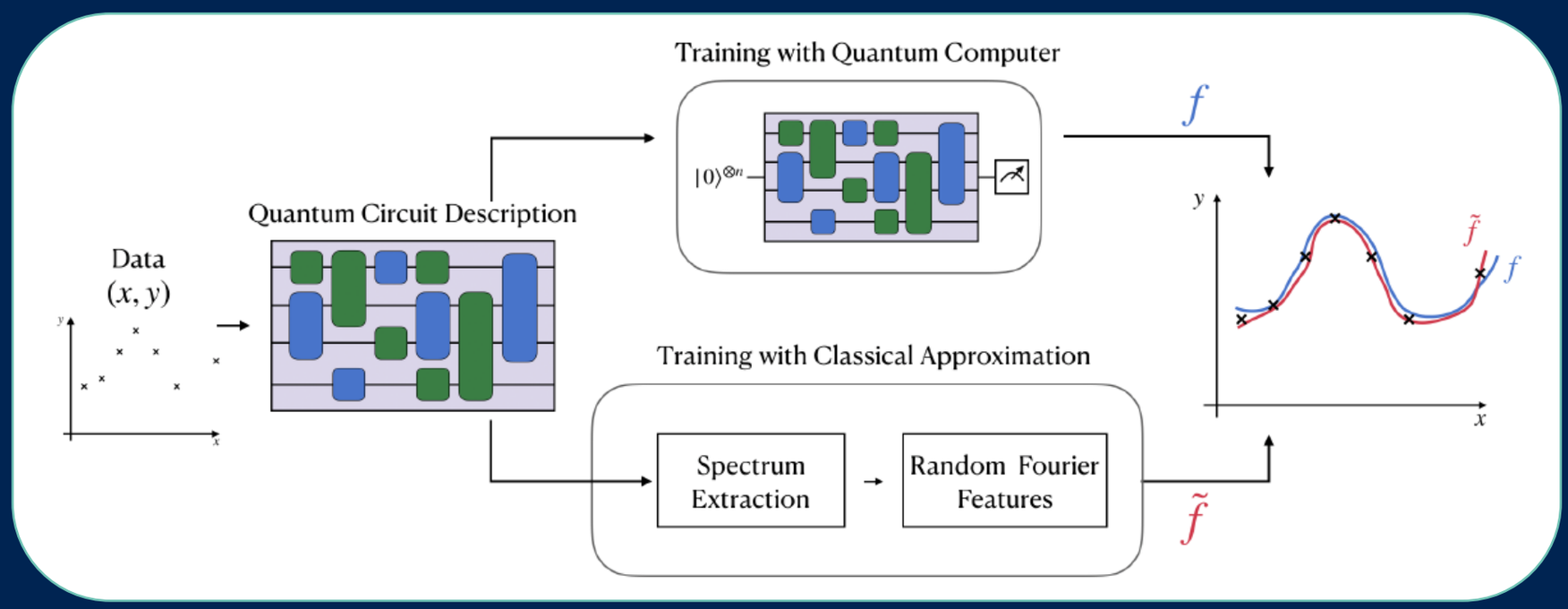
Privacy Preserving
QML in Cloud Using
QLine

When quantum machine learning offers a practical advantage?

When quantum machine learning offers a practical advantage?



Variational Quantum Circuits give rise to Fourier Series

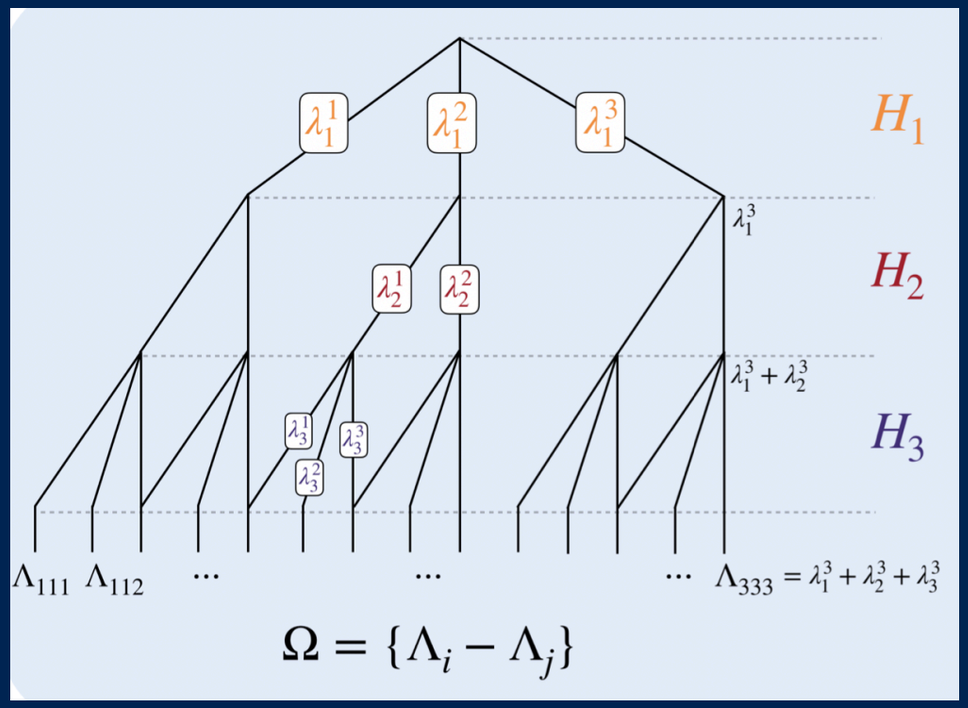


Landman et.al. arXiv:2210.13200

Expressivity

Data Encoding

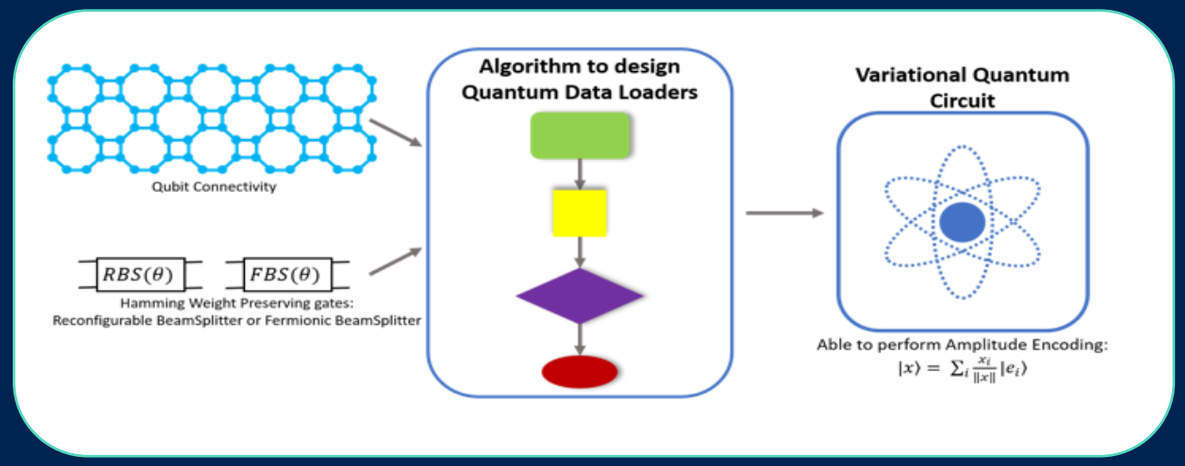
Expressivity



From encoding Hamiltonians to Frequencies

Guidelines on how to design quantum circuits for particular tasks

Data Encoding



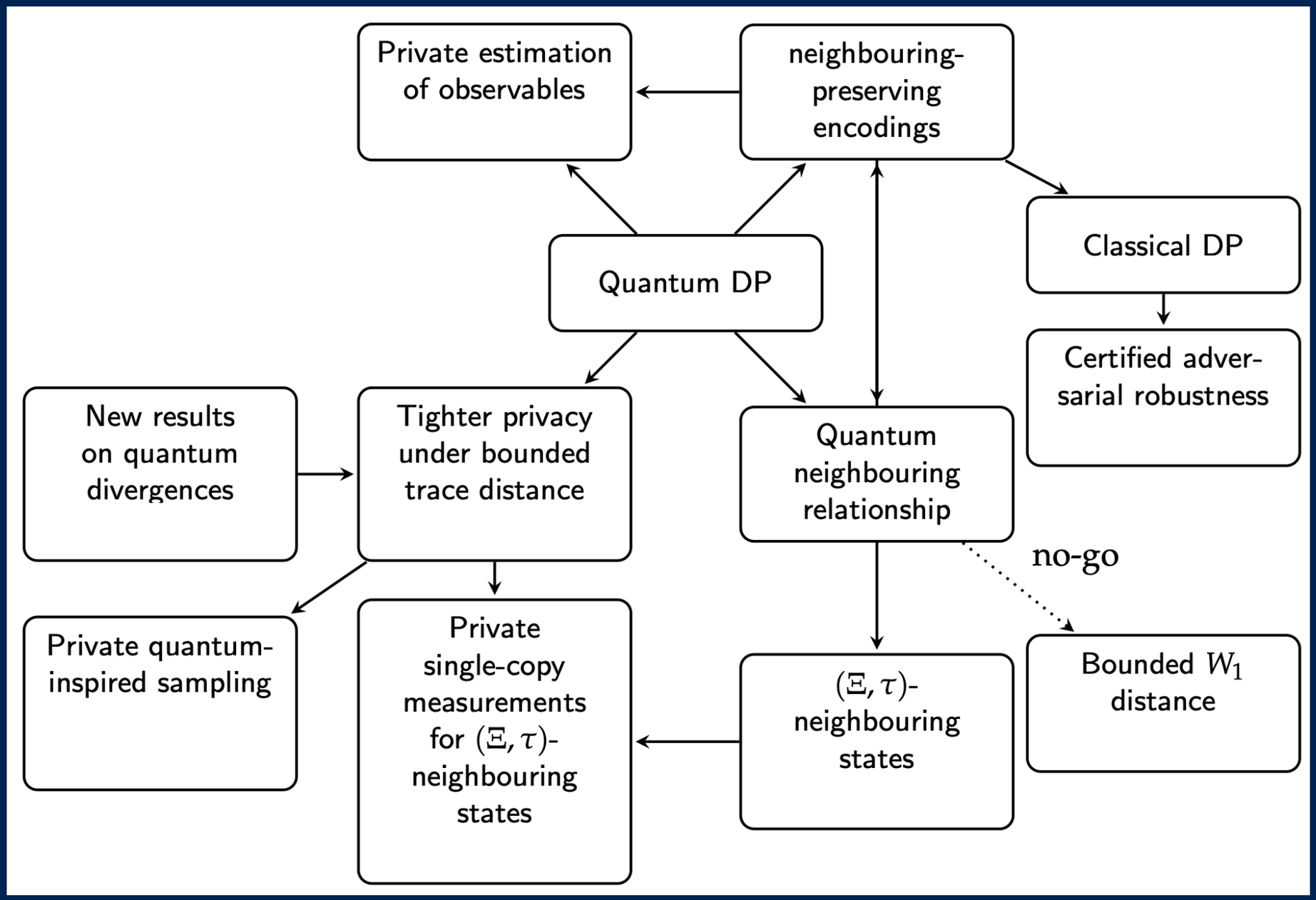
Dynamical Lie Algebra

Framework for Quantum Data Loader design with proven trainability

Monbroussou et.al. arXiv:2309.15547

How can we hide quantum data with classical Differential Privacy?

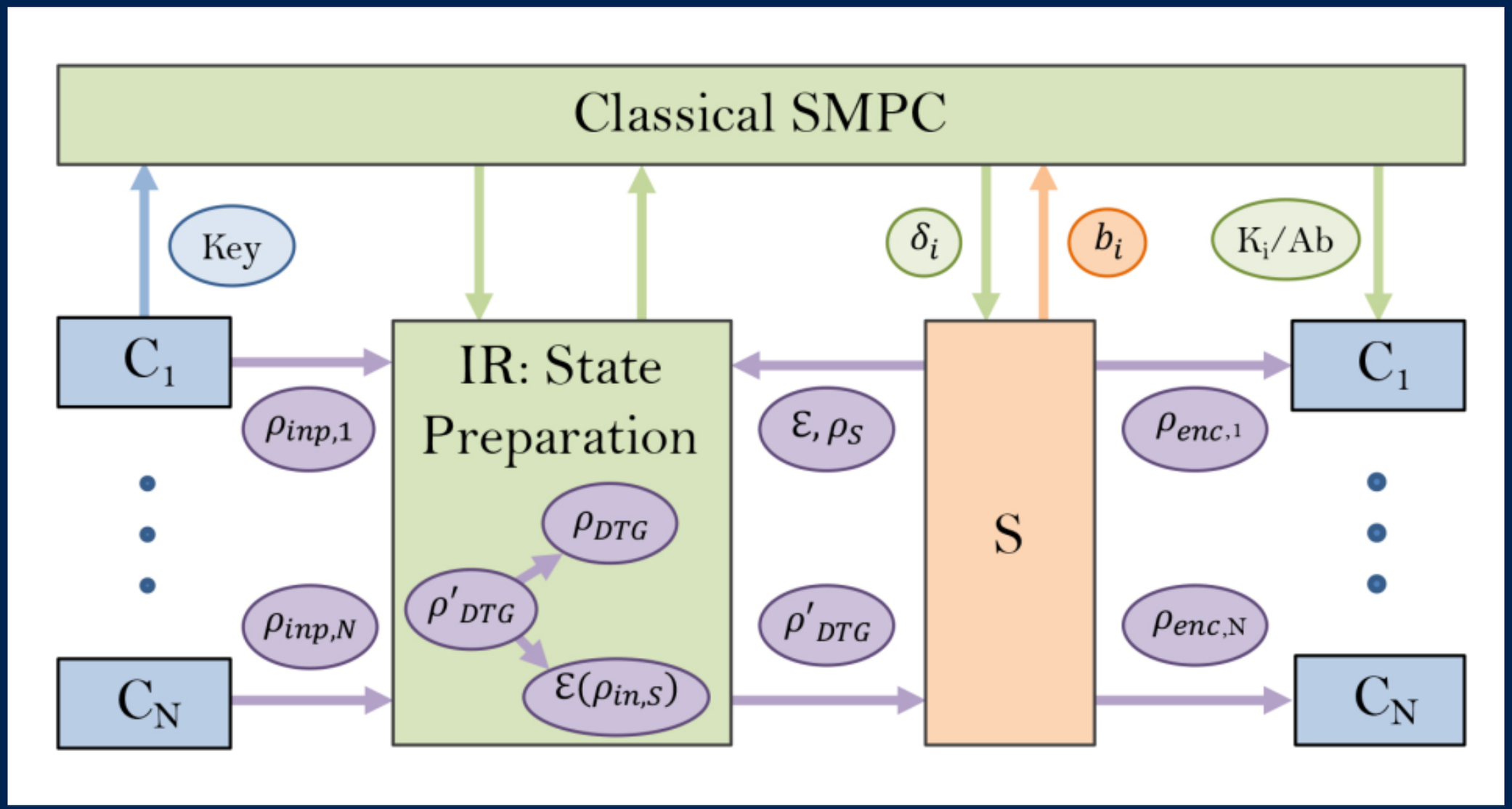
How can we hide quantum data with classical Differential Privacy?



Angrisani et.al. arXiv:2307.04733

How can we hide quantum data with classical Secure Multi Party Computing?

How can we hide quantum data with classical Secure Multi Party Computing?



Kapourniotis et.al. arXiv:2303.08865

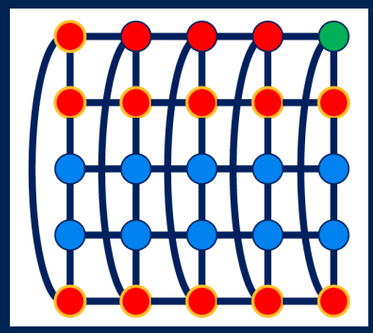
How to handle hardware noise for current devices ?

How to handle hardware noise for current devices ?

Decoupling Verifiability and Fault-Tolerance

(T, σ, τ) on graph G = (V, E)

- T = sub-computation (pattern + flow)
- σ = fixed input
- τ = decision function on outputs



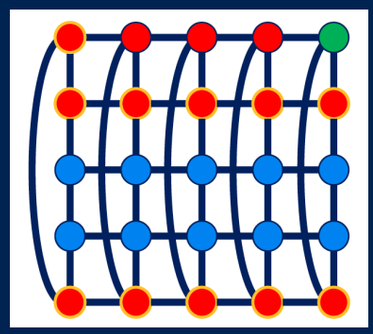
Leichtle et.al. arXiv:2206.00631

How to handle hardware noise for current devices ?

Decoupling Verifiability and Fault-Tolerance

(T, σ, τ) on graph G = (V, E)

- T = sub-computation (pattern + flow)
- σ = fixed input
- τ = decision function on outputs



new trap schemes = probabilistic error-detecting schemes = Linear programming

Given

- a set of errors $\mathcal{E}$ to be detected,
- a set of feasible tests $\mathcal{H}$,
- a relation between tests and errors describing whether a test detects an error, $R : \mathcal{H} \times \mathcal{E} \to \{0, 1\}$,

find an optimal distribution $p : \mathcal{H} \to [0, 1]$ **maximising** the detection rate $\epsilon \in [0, 1]$ **subject to** the following conditions:

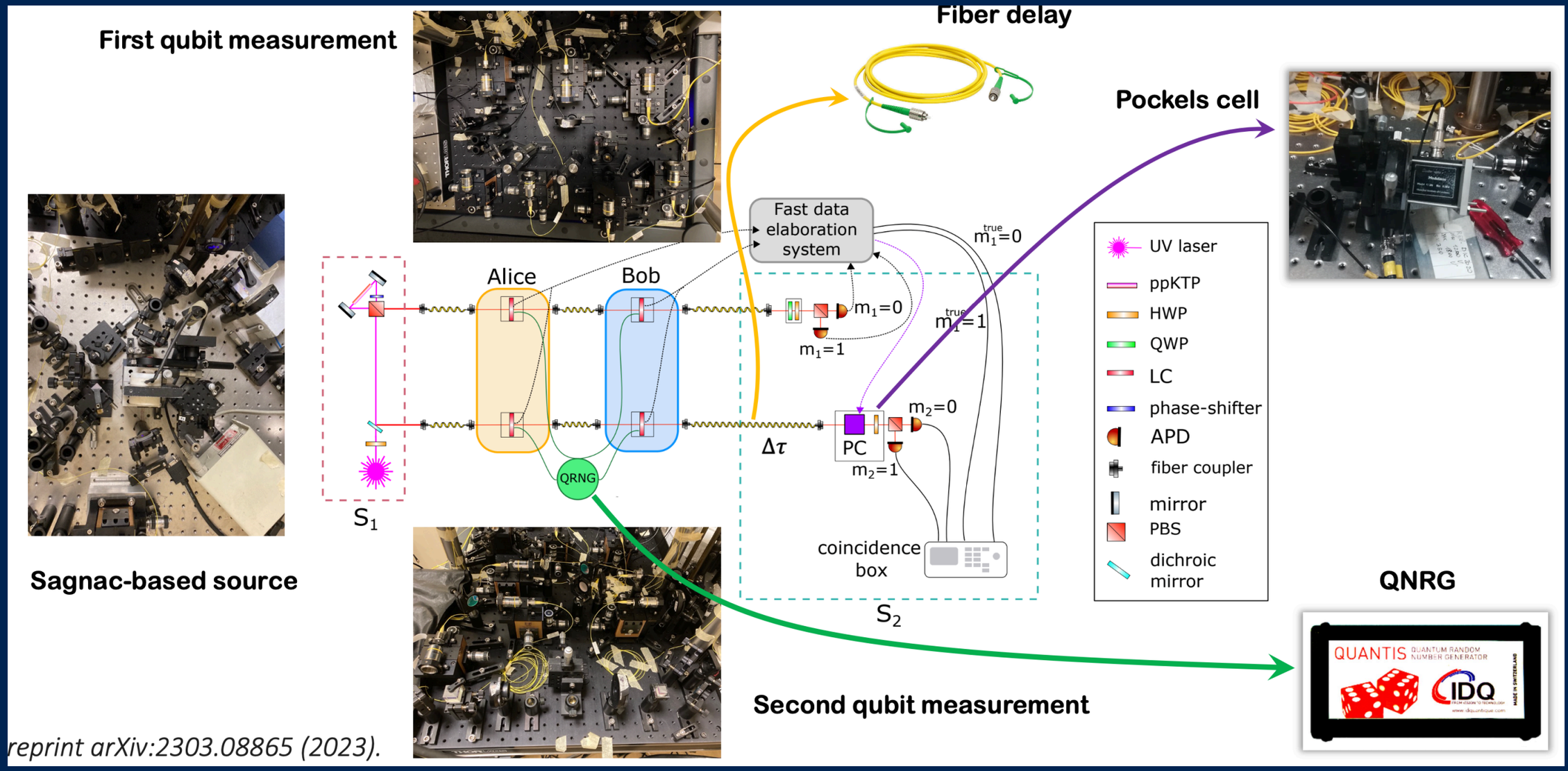
- p describes a probability distribution, i.e. $\sum_{H \in \mathcal{H}} p(H) \leq 1$,
- all concerned errors are detected at least with the target detection rate, i.e.

$$\forall E \in \mathcal{E} : \quad \sum_{\substack{H \in \mathcal{H} \\ R(H,E)=1}} p(H) \geq \epsilon.$$

Leichtle et.al. arXiv:2206.00631

Can we build it now ?

Can we build it now ?



reprint arXiv:2303.08865 (2023).

quantum memory = trusted execution module

Polacchi et.al. arXiv:2306.05195

Quantum Utopia

It takes the entire *classical ICT research* to raise a *useful* quantum application

Quantum Software Lab