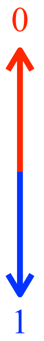
Quantum Leap
in Next-Generation Computing

(WSO2Con, Miami, FL, USA, May 7 - 9, 2024)

Prof. Dr. Dr. h.c. Frank Leymann
WSO2 Technology Fellow
University of Stuttgart, Germany

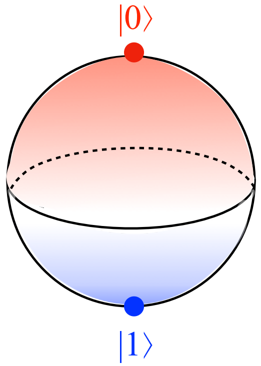
Why?

Qubit vs. Bit: The Fundamental Difference



Bit

A bit is either "0" or "1"
→ Two possible values



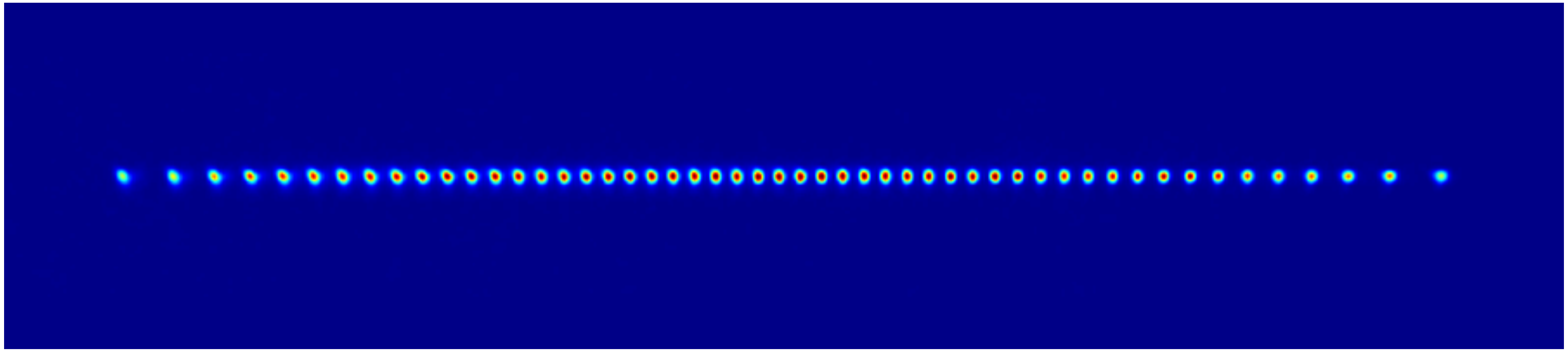
Qbit

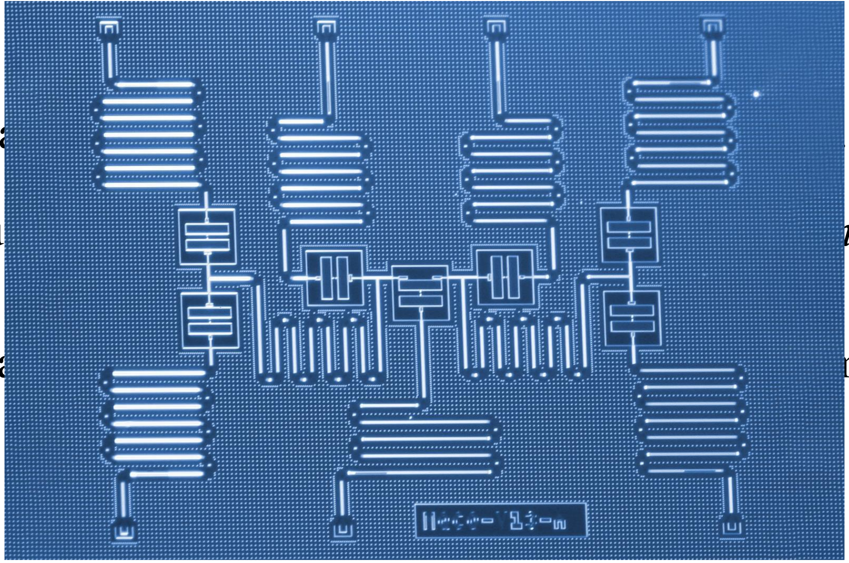
A qubit is an arbitrary point
on this "Bloch sphere"
→ Infinitely many possible values

…Combination of $|0\rangle$ and $|1\rangle$ at the same time:

$$\alpha|0\rangle + \beta|1\rangle$$

The Power of a Quantum Register





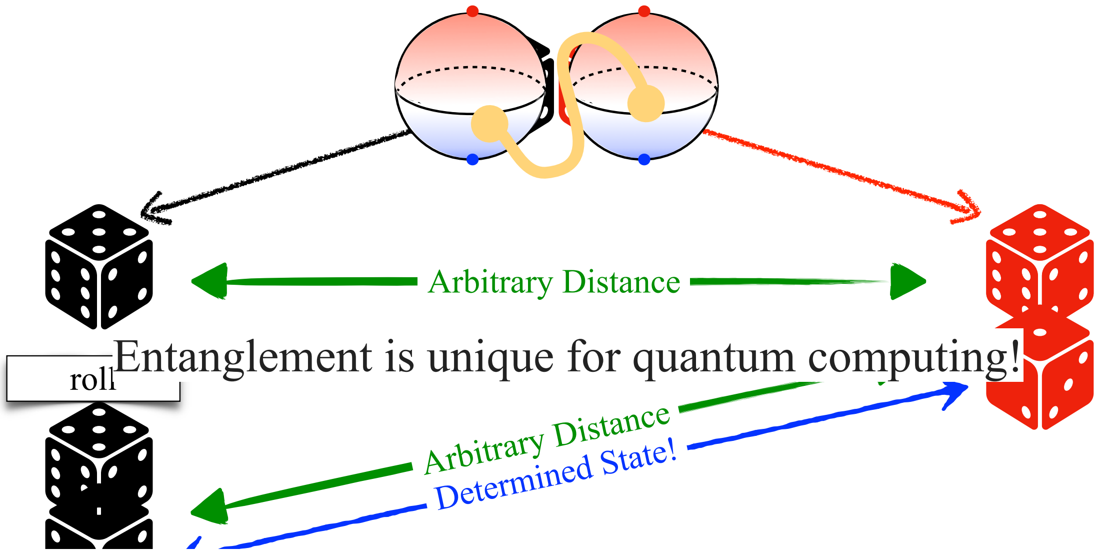
(the va …1⟩)

#atoms in u n=300 Qbits

…a ne!

IBM has ≈ **400 qubits** commercially available

Entanglement: The Miracle



Entanglement is unique for quantum computing!

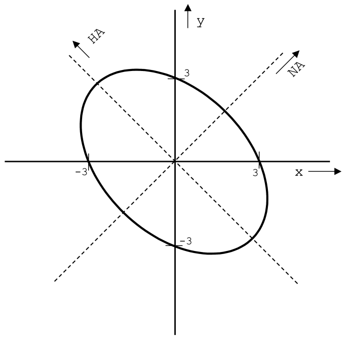
Every quantum algorithm showing exponential speedup compared to classical algorithms, must exploit entanglement.

Impact

- Several problems that can not be solved efficiently on a classical computer can be solved efficiently (or with higher precision) on a quantum computer
  - E.g. there are polynomial quantum algorithms for problems for which only exponential classical algorithms are known
- This allows to solve problems that can’t be solved classically by now in practice (or only "badly")
- This enables e.g. new business models

Example:
Efficient Quantum Algorithms

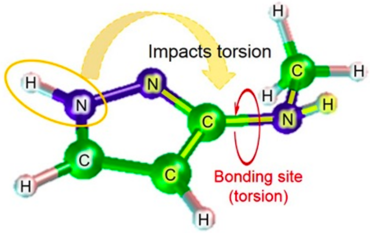
Computing Eigenvalues
⇒ E.g.: Feature Engineering



Factorization
⇒ E.g.: Cracking Keys

$$\begin{aligned} & 18018 \\ = \; & \overbrace{2 \cdot 9009} \\ = \; & 2 \cdot \overbrace{3 \cdot 3003} \\ = \; & 2 \cdot 3 \cdot \overbrace{3 \cdot 1001} \\ = \; & 2 \cdot 3 \cdot 3 \cdot \overbrace{7 \cdot 143} \\ = \; & 2 \cdot 3 \cdot 3 \cdot 7 \cdot \overbrace{11 \cdot 13} \end{aligned}$$

Molecule Simulation
⇒ E.g.: Material Science



Linear Equation Systems
⇒ E.g.: Machine Learning

$$A \cdot x = b$$

Example:
New Applications & Business Models

- Manufacturing: Solving optimization problems
  - Scheduling, transport & logistics, robot movement,…
- Product simulation: Solving linear equation systems
  - Stability of objects, combustion processes in engines & turbines,…
- Material science: Eigenvalue computations
  - Catalysts for batteries, new pharmaceuticals, personalized medicine,…

Quantum Machine Learning

- Classical No-Free-Lunch theorem of supervised learning

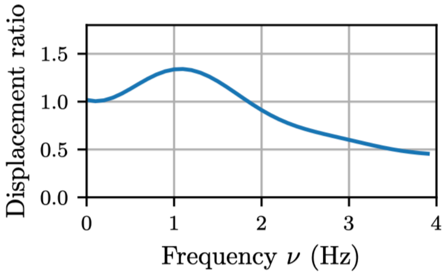
The more training data is used,
the lower the average error in learning a neural net

- Quantum No-Free-Lunch theorem of supervised learning

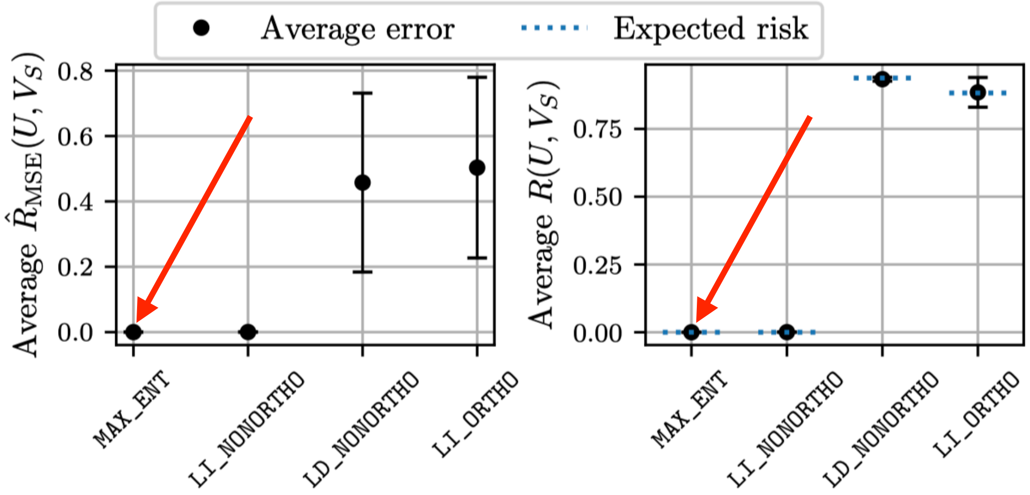
The more the training data is entangled,
the less training data is needed
to learn a quantum neural net with low average error

A ***single*** pair of maximally entangled training data suffice,
to train a quantum neural net with low average error
("in high dimensions")

Example: Damper Parameterization



- Predictor for chassis movement of a car driving on a bumpy road
  - …known from practice by an automotive company
- Use a quantum neural net to learn this predictor
  - …using a simplified car model



- Used training data of various entanglement strengths
- Use of maximally entangled data learned the correct predictor

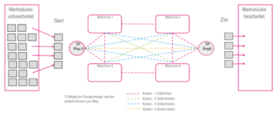
Quantum Optimization

- Combinatorial optimization problems
  - Quadratic Binary Optimization (QUBO)

- Examples: gate assignment, task allocation, clustering,…

- Traveling Salesman Problem

- Dynamic Traveling Salesman Problem

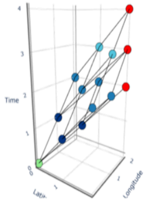


Wolfgang Steigerwald

Job Scheduling Optimization

AXOVISION

Financial Portfolio Optimization via QUBOs



Fabian Klos

Multi-Aircraft-Routing

Marc Geitz

Customer Relationship Management

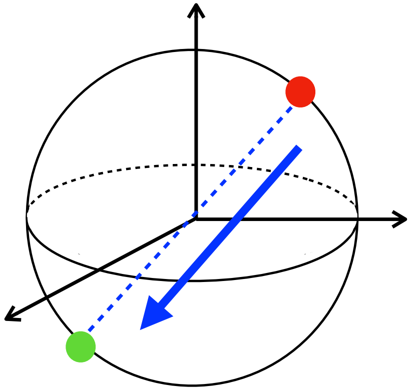
Anaqor AG

Fleet Route Planning

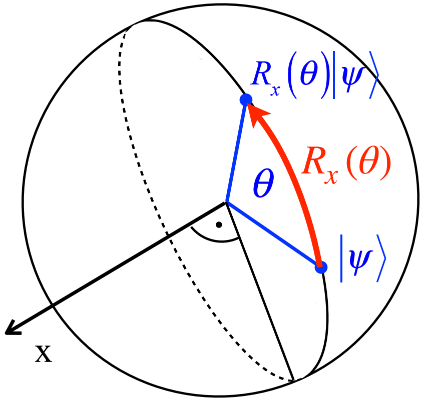
Note:
All implemented use cases
have a "small" size

When?

We are in the NISQ Era



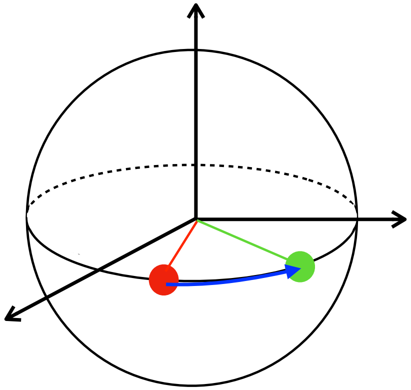
Relaxation:
spontaneous transition
into diametral state



Decoherence

Operation Errors:
rotation is a little imprecise
[can’t rotate an exact angle]

Fidelity



Dephasing:
Minor disturbances or trembling

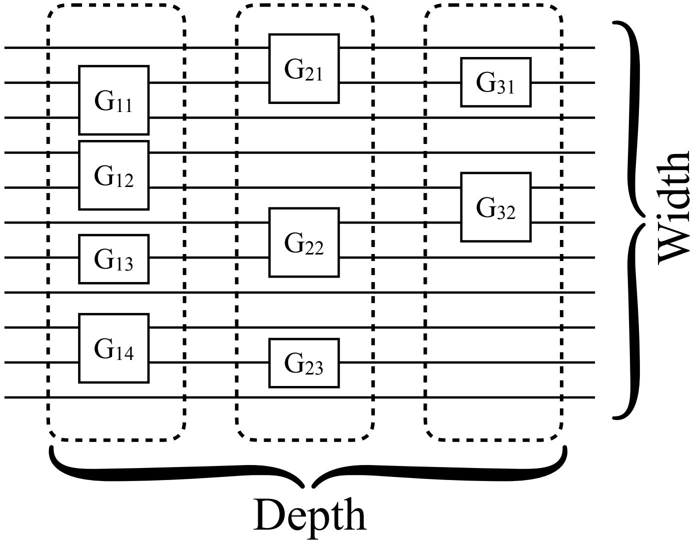
NISQ: **N**oisy **I**ntermededate **S**cale **Q**uantum

Consequence of NISQ

- Noise means that errors pile up over time
  ⇒ algorithms must be "small"
  - Few qubits or few parallel layers
  - More precise: *width* × *depth* << *error-rate*

- Ideal: many qubits ⇒ no classical simulation possible!
  ⇒ quantum advantage possible
  Thus, today's implementations should have low depth

- But "pumping" data into QC takes time
  - First part of an algorithm must prepare the input data
    ⇒ only "small" amount of data can be processed



Manipulating Qubits

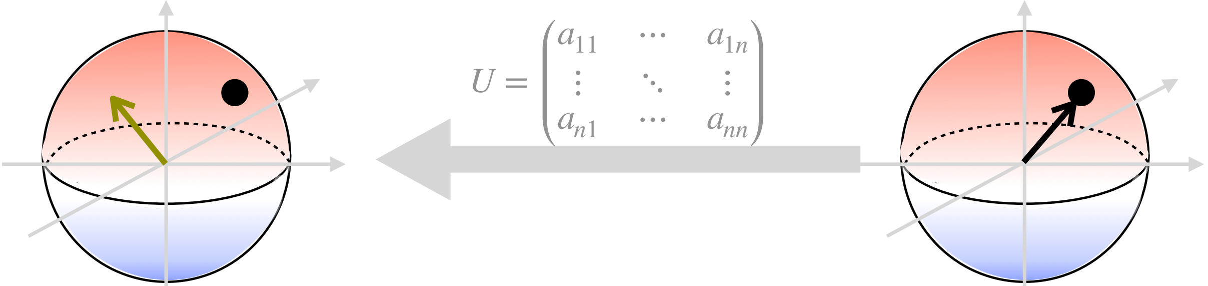
Remember: a qubit q is a combination of $|0\rangle$ and $|1\rangle$ at the same time, i.e. $q = \alpha|0\rangle + \beta|1\rangle$

- $|\alpha|^2$: probability of being $|0\rangle$
- $|\beta|^2$: probability of being $|1\rangle$

Thus, $|q|^2 = |\alpha|^2 + |\beta|^2 = 1$ - which means q is vector of length 1

Manipulating a qubit means

- to turn a vector of length 1
- into another vector of length 1



$$U = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

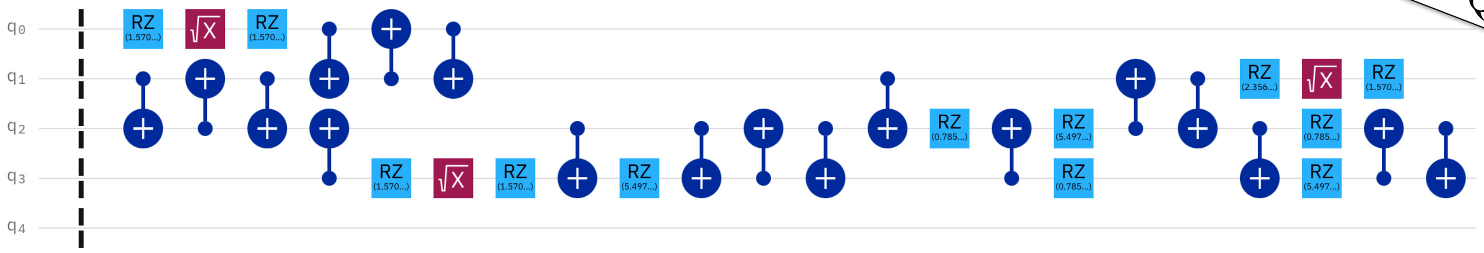
Such length-preserving (linear) maps are called "unitary"

Thus, quantum algorithms consists of series of unitary maps (matrices)

≈ Rotations of a qubit on the Bloch sphere

Learning Curve: Quantum Programming

- Programming a quantum computer is very different from classical programming
  - Linear algebra in complex vector spaces



Quantum Circuit

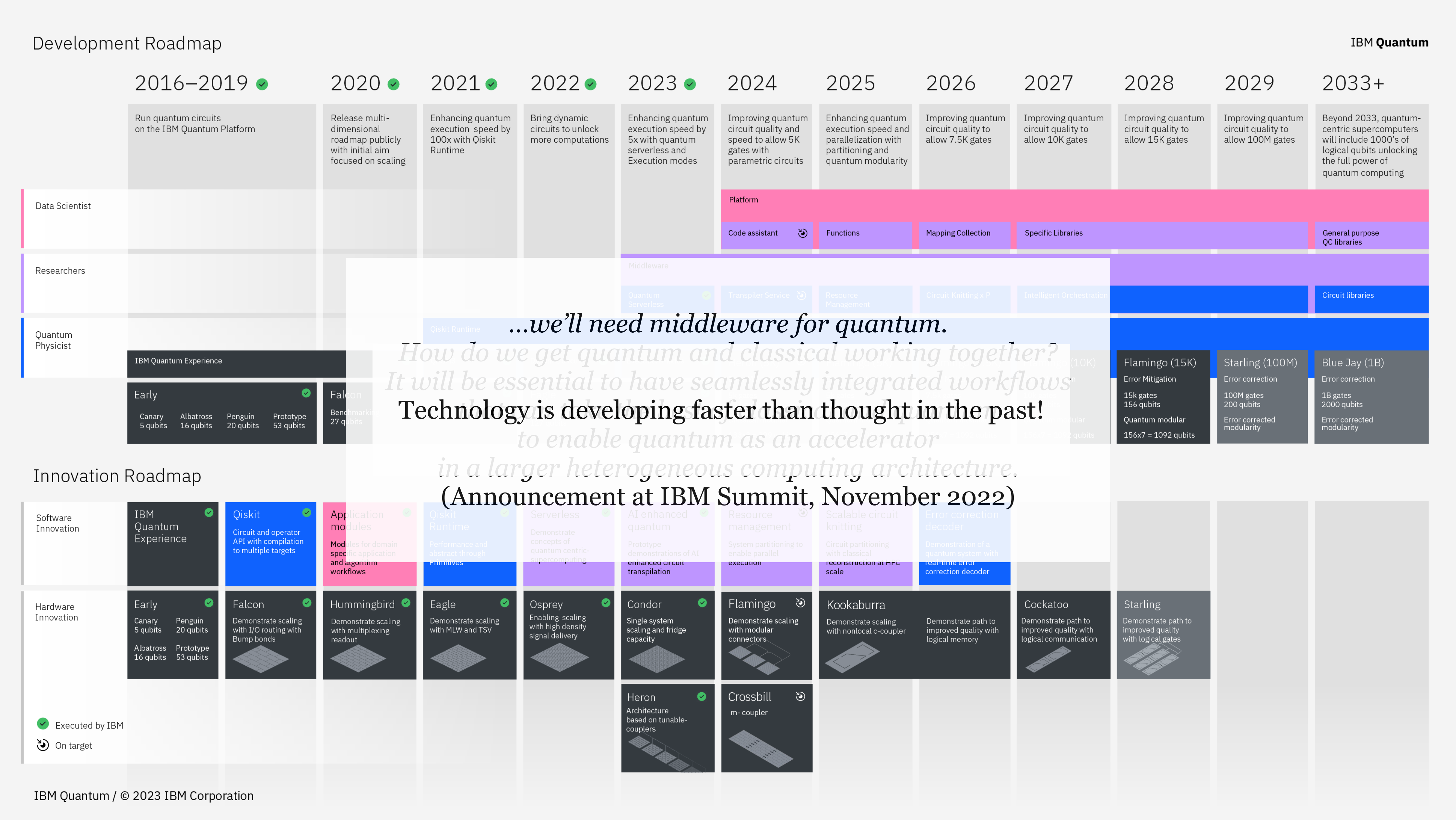
- **Skill development takes time**

- But quantum computing technology is currently developing faster than predicted!

⇒ If you don't start now, you run the risk of being left behind!

?

How?



Development Roadmap

IBM **Quantum**

2016–2019 ✓	2020 ✓	2021 ✓	2022 ✓	2023 ✓	2024	2025	2026	2027	2028	2029	2033+
Run quantum circuits on the IBM Quantum Platform	Release multi-dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum execution speed and parallelization with partitioning and quantum modularity	Improving quantum circuit quality to allow 7.5K gates	Improving quantum circuit quality to allow 10K gates	Improving quantum circuit quality to allow 15K gates	Improving quantum circuit quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing

Data Scientist

Platform

Code assistant | Functions | Mapping Collection | Specific Libraries | General purpose QC libraries

Researchers

Middleware

Quantum Serverless ✓ | Transpiler Service | Resource Management | Circuit Knitting x P | Intelligent Orchestration | Circuit libraries

Quantum Physicist

Qiskit Runtime

IBM Quantum Experience

Early ✓ — Canary 5 qubits, Albatross 16 qubits, Penguin 20 qubits, Prototype 53 qubits

Falcon — Benchmarking 27 qubits

(10K)

Flamingo (15K) — Error Mitigation; 15k gates 156 qubits; Quantum modular; 156x7 = 1092 qubits

Starling (100M) — Error correction; 100M gates 200 qubits; Error corrected modularity

Blue Jay (1B) — Error correction; 1B gates 2000 qubits; Error corrected modularity

Innovation Roadmap

Software Innovation

- IBM Quantum Experience ✓
- Qiskit ✓ — Circuit and operator API with compilation to multiple targets
- Application modules ✓ — Modules for domain specific application and algorithm workflows
- Qiskit Runtime ✓ — Performance and abstract through Primitives
- Serverless ✓ — Demonstrate concepts of quantum centric-supercomputing
- AI enhanced quantum ✓ — Prototype demonstrations of AI enhanced circuit transpilation
- Resource management — System partitioning to enable parallel execution
- Scalable circuit knitting — Circuit partitioning with classical reconstruction at HPC scale
- Error correction decoder — Demonstration of a quantum system with real-time error correction decoder

Hardware Innovation

- Early ✓ — Canary 5 qubits, Penguin 20 qubits, Albatross 16 qubits, Prototype 53 qubits
- Falcon ✓ — Demonstrate scaling with I/O routing with Bump bonds
- Hummingbird ✓ — Demonstrate scaling with multiplexing readout
- Eagle ✓ — Demonstrate scaling with MLW and TSV
- Osprey ✓ — Enabling scaling with high density signal delivery
- Condor ✓ — Single system scaling and fridge capacity
- Heron ✓ — Architecture based on tunable-couplers
- Flamingo — Demonstrate scaling with modular connectors
- Crossbill — m- coupler
- Kookaburra — Demonstrate scaling with nonlocal c-coupler; Demonstrate path to improved quality with logical memory
- Cockatoo — Demonstrate path to improved quality with logical communication
- Starling — Demonstrate path to improved quality with logical gates

✓ Executed by IBM

On target

IBM Quantum / © 2023 IBM Corporation

…we'll need middleware for quantum.

How do we get quantum and classical working together?

It will be essential to have seamlessly integrated workflows

Technology is developing faster than thought in the past!

to enable quantum as an accelerator

in a larger heterogeneous computing architecture.

(Announcement at IBM Summit, November 2022)

Setup

- Solutions using quantum algorithms always require classical software too
  - Quantum applications are *hybrid*

    ⇒ need to use integration technologies (workflows,…)

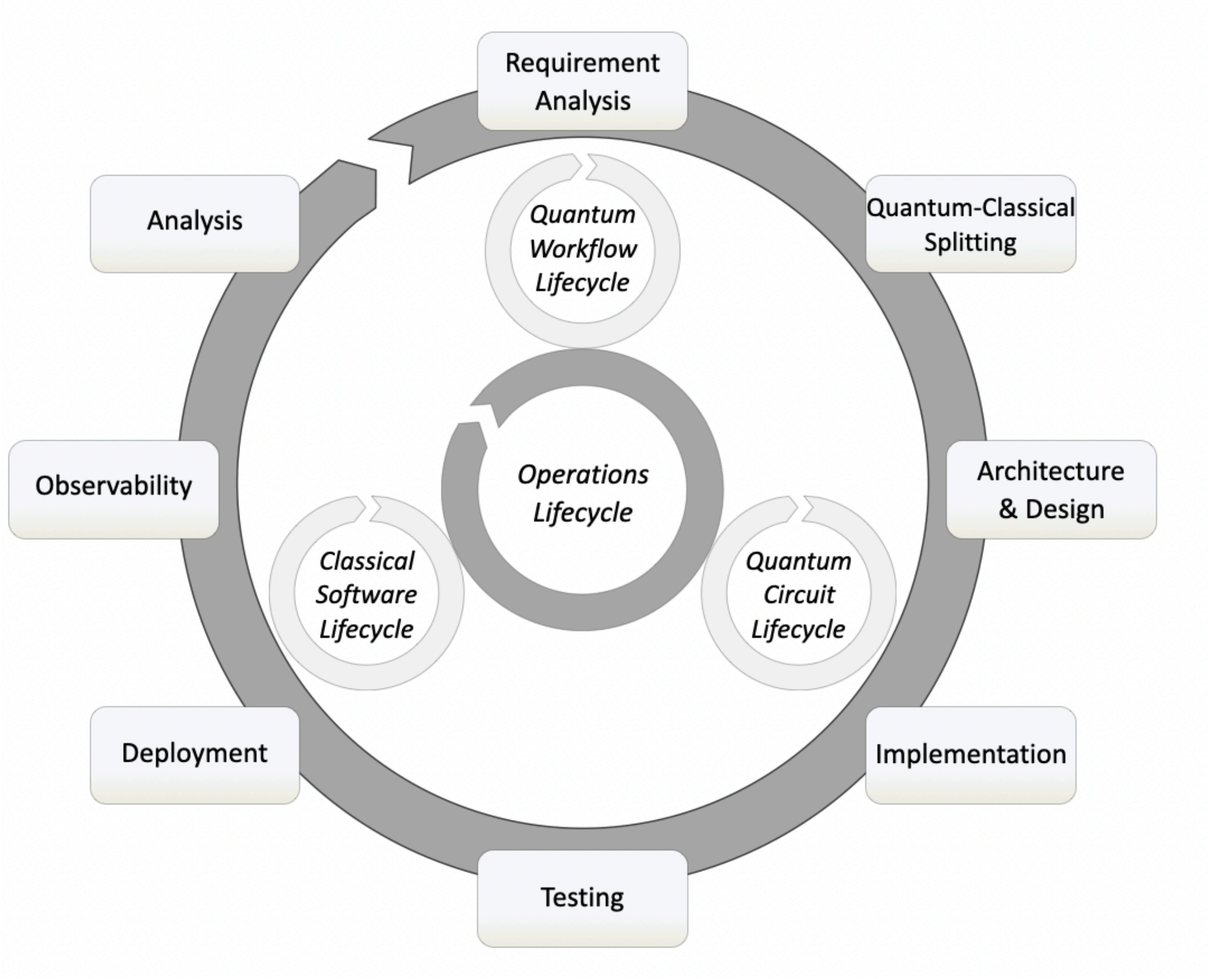
- Development of successful quantum applications require a team of...
  - …classical programmers, integration specialists, quantum algorithm programmers

    ⇒ built a corresponding team

- Utility assessed based on a business-related problems that you can’t solve today
  - Analyze existing quantum algorithms for indicating advantage over classical algorithms
  - Implement corresponding quantum application

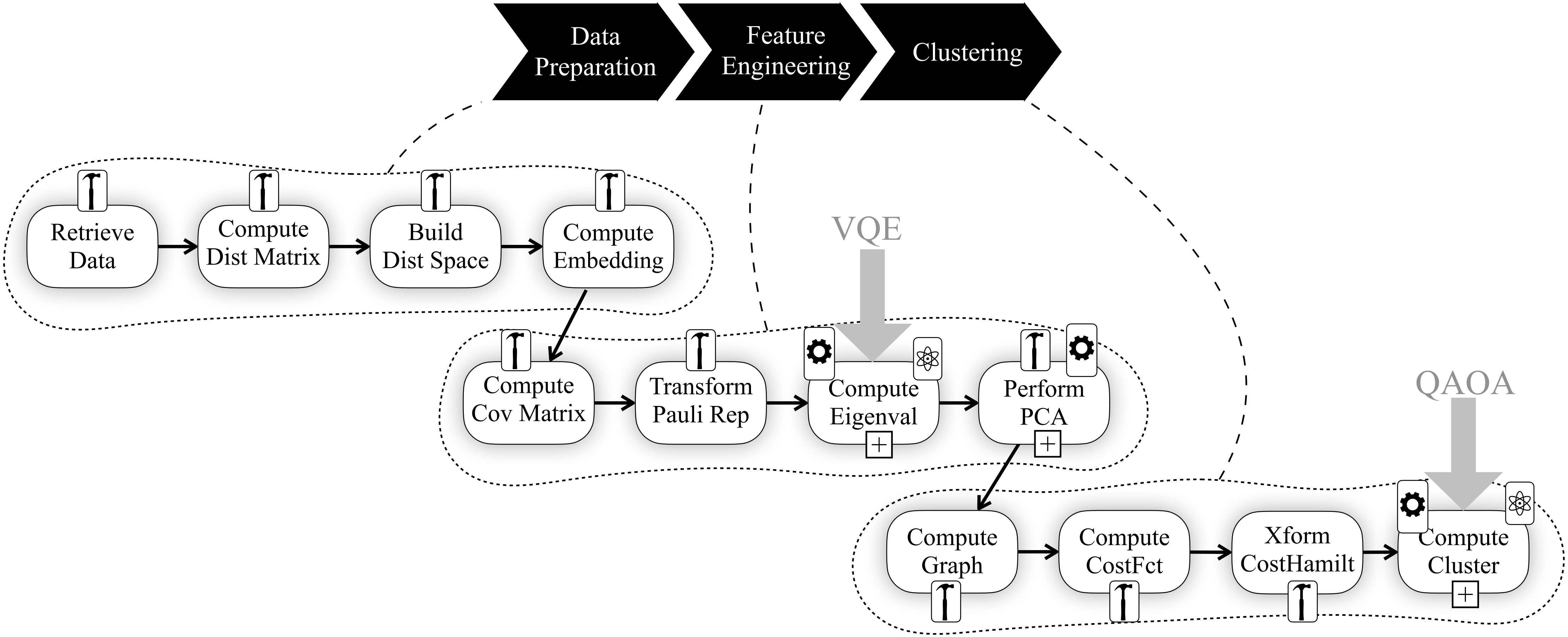
    ⇒ Assessment of solution based on vendor roadmap

Developing Quantum Applications

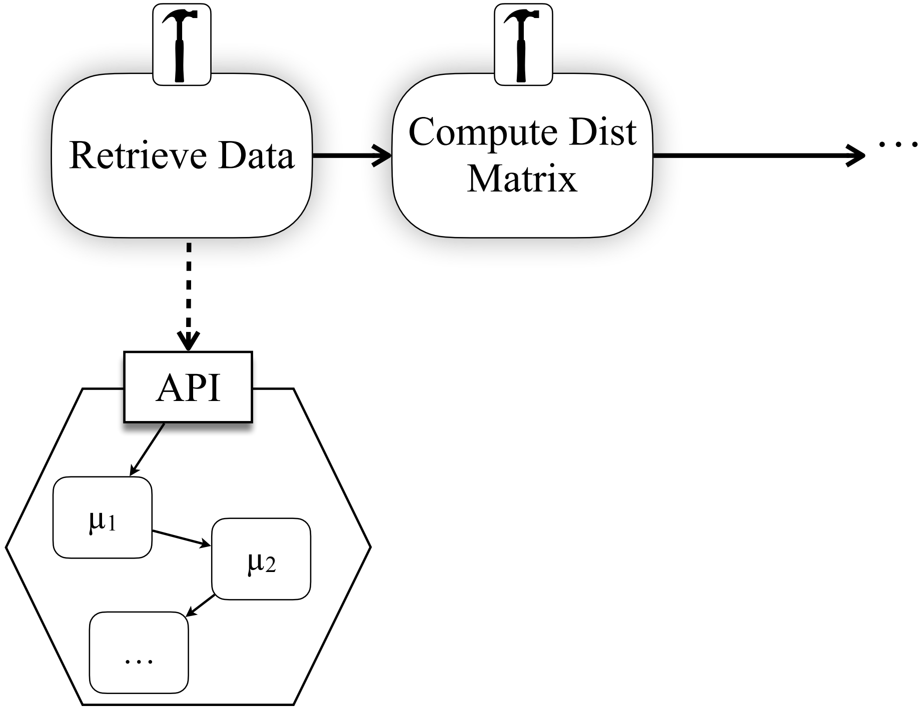


© Frank Leymann

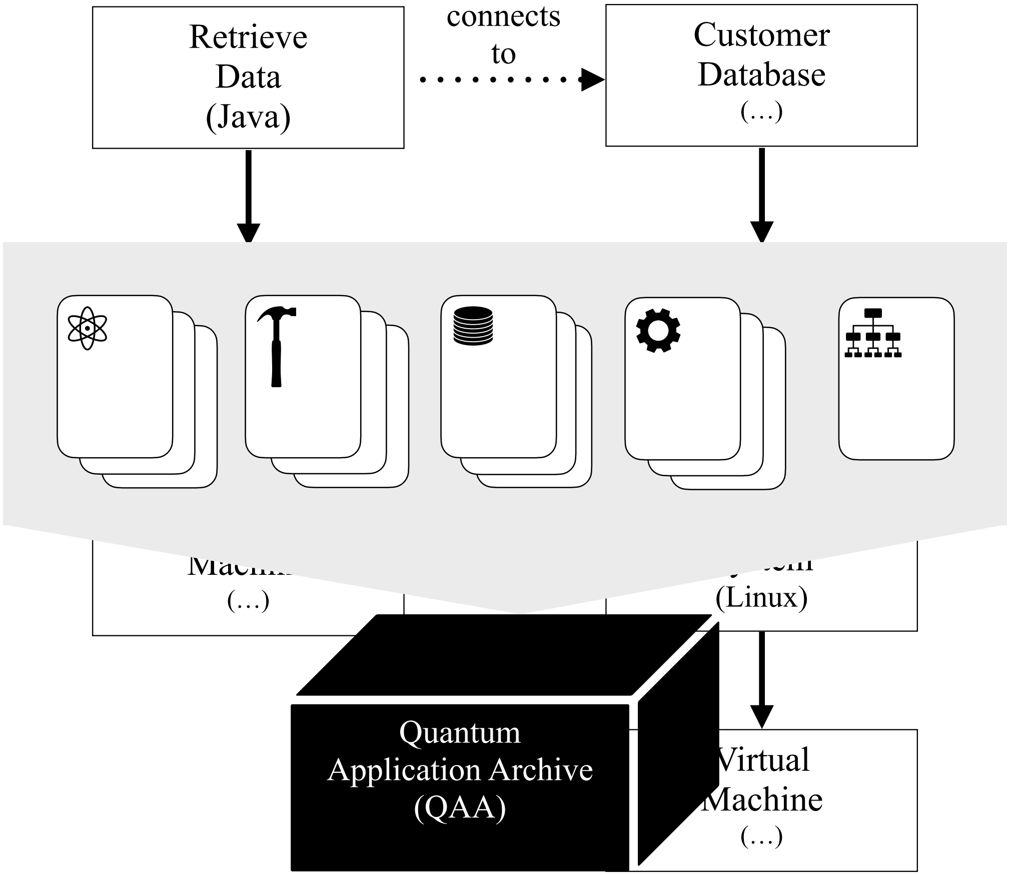
Example: Quantum Machine Learning



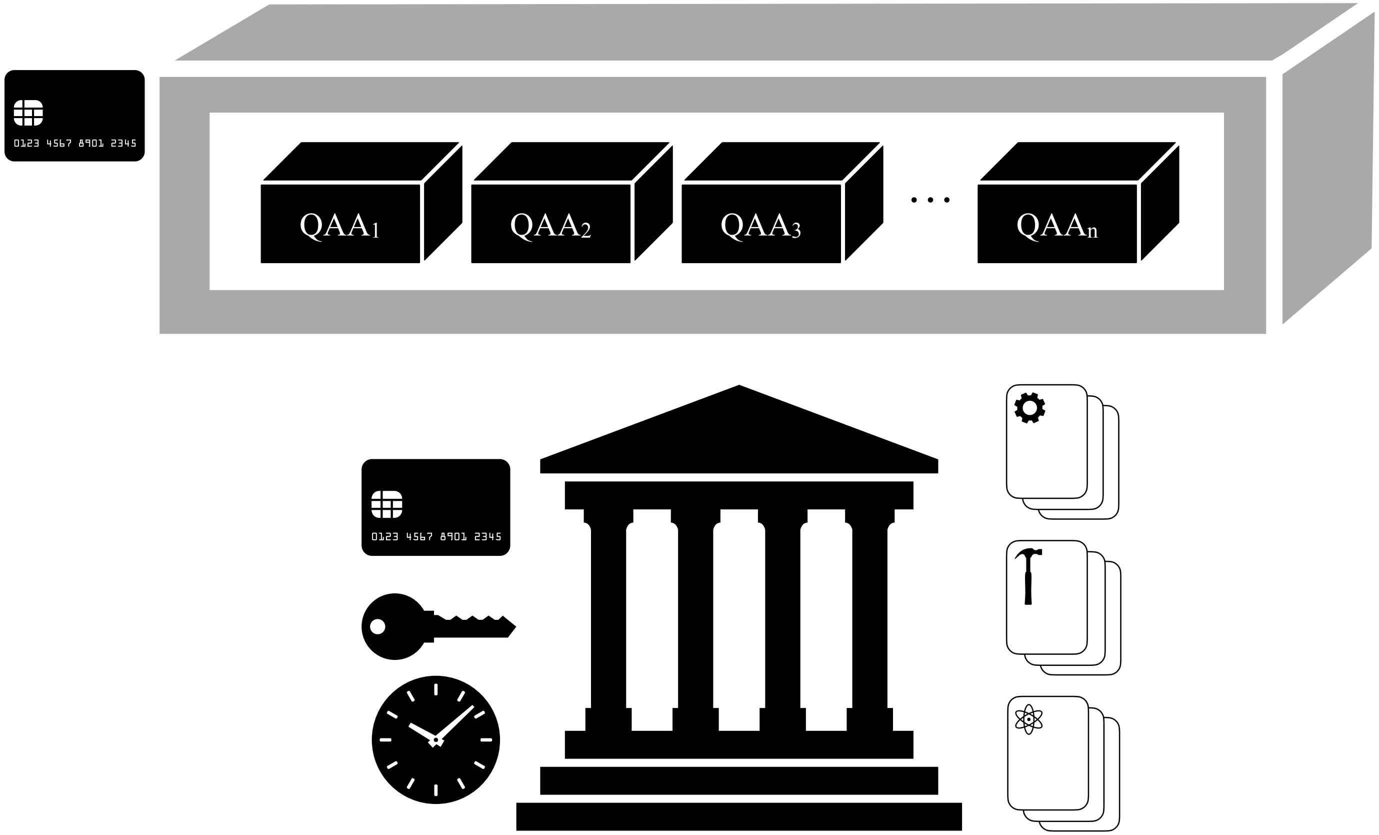
The Role of APIs, (Micro-)Services, Cells,…



Packaging and Deployment

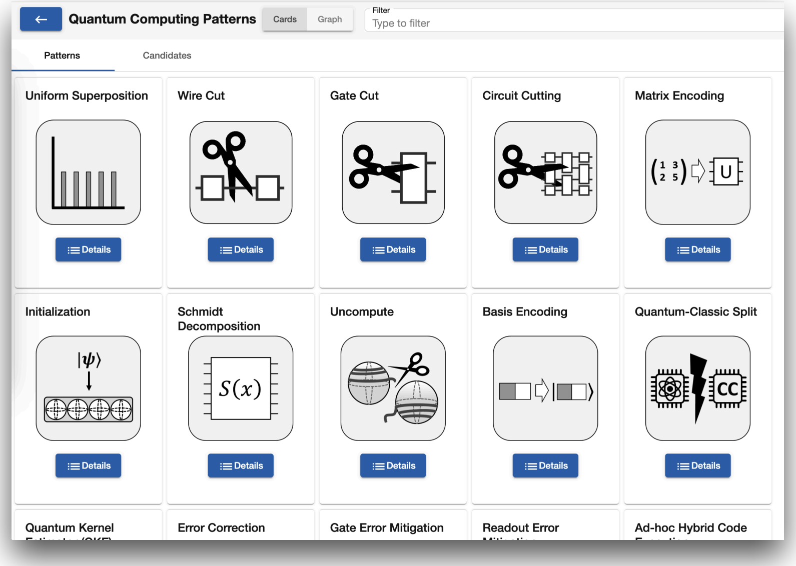


AppStore & API Management

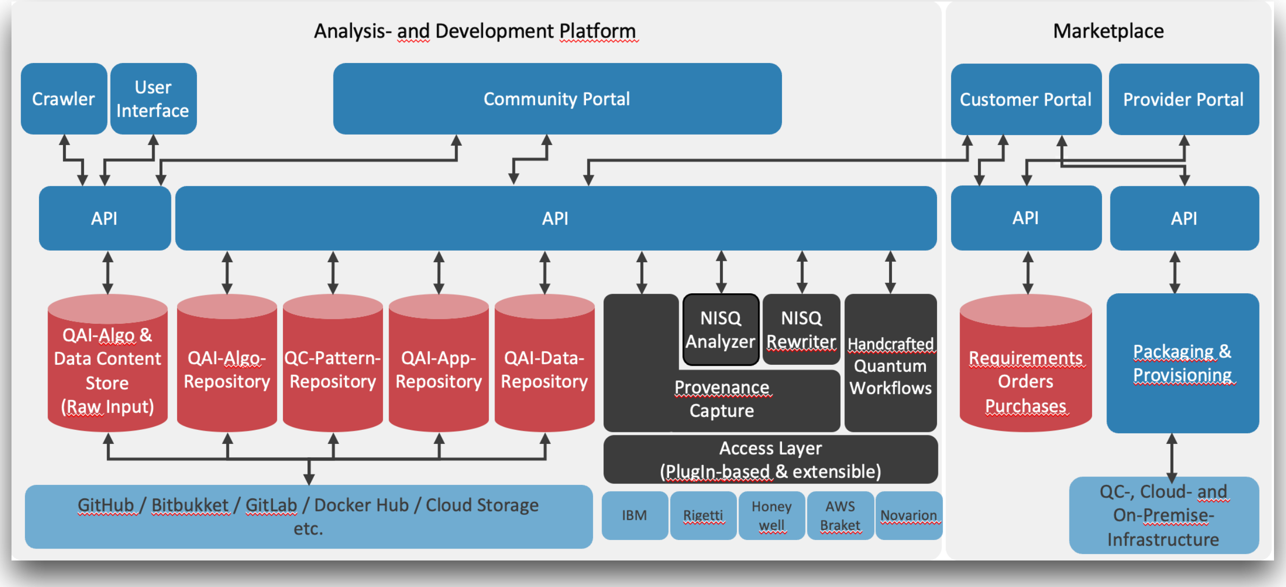


Remember:
Skill Development Takes Time

- Reusing experiences and proven solutions is very welcome ⇒ Pattern language for quantum computing
- Tools for developing and executing quantum applications are very welcome



https://patterns.platform.planqk.de/pattern-languages



Analysis- and Development Platform

Marketplace

Crawler

User Interface

Community Portal

Customer Portal

Provider Portal

API

API

API

API

QAI-Algo & Data Content Store (Raw Input)

QAI-Algo-Repository

QC-Pattern-Repository

QAI-App-Repository

QAI-Data-Repository

NISQ Analyzer

NISQ Rewriter

Handcrafted Quantum Workflows

Provenance Capture

Access Layer (PlugIn-based & extensible)

Requirements Orders Purchases

Packaging & Provisioning

GitHub / Bitbukket / GitLab / Docker Hub / Cloud Storage etc.

IBM

Rigetti

Honey well

AWS Braket

Novarion

QC-, Cloud- and On-Premise-Infrastructure

https://platform.planqk.de/home

Threat!

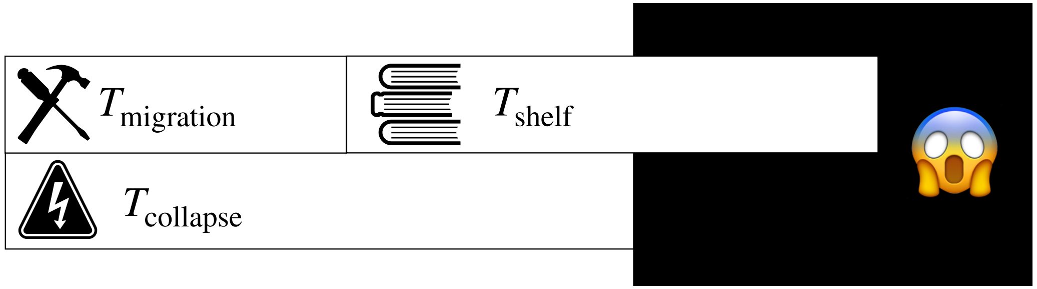
Post-Quantum Cryptography

- Quantum algorithm exists that can solve the *discrete logarithm problem* in polynomial time!

- Thus, a (future!) quantum computer can crack today's cryptography based on, e.g., …
  - …prime factorization (e.g. RSA)
  - …elliptic curves (e.g. ECDH)

- Rescue is lattice-based cryptography
  - Currently standardized by NIST
  - Algorithms which can not be cracked as of today (!) classically or quantum

Are You Safe?



$T_{\text{migration}}$

T_{shelf}

T_{collapse}

You are in trouble if: $T_{\text{shelf}} + T_{\text{migration}} > T_{\text{collapse}}$ (Mosca's Inequality)

Assume $T_{\text{collapse}} = 10\ \text{y}$, $T_{\text{shelf}} = 10\ \text{y}$ $\Rightarrow$ $T^{\text{max}}_{\text{migration}} = 0\ \text{y}$ **You must begin now!**

But WSO2 is Acting Already

Prototypes are under way

- Communication between **Ballerina** services is about to become quantum safe
  - Also, crypto API extension to support PQC
- **Identity Server** (on prem) and **Asgardeo** is about to become quantum safe
  - Inbound/outbound communication
  - Data stored
  - Transmission of tokens is about to become quantum safe

Closing…

First To Note

- Quantum computers are specialized devices
  - E.g., don’t expect a quantum mobile phone any time soon 😌

- There impact in everyday life will be subtle, not immediately noted by everyone
  - Personalized drugs, long-lasting batteries, highly precise navigation, etc etc etc

- But: Cryptography threat!

Take Aways

- Quantum computers are real
  - …with a very different programming model
  - New applications and new business models are at the horizon
- Quantum applications are hybrid
  - …i.e. a mixture of classical programs and quantum programs
  - Building quantum applications is an integration problem
- Existing software lifecycles need to be extended to include quantum
  - …and produce tradable artifacts
- Quantum applications can be deployed and executed on premise or in a cloud environment or mixed
- There is a security threat
  - WSO2 is already acting

Conclusion:
Quantum Computing…

Why?

Previously unrealizable and completely new business models appear possible

When?

Begin now!

How?

Skill development ↦ problem identification ↦ systematic engineering ↦ assessment

Quote by Enrico Fermi

I am still confused…

…but at a higher level!

The End