Post-Quantum

Cryptography Conference

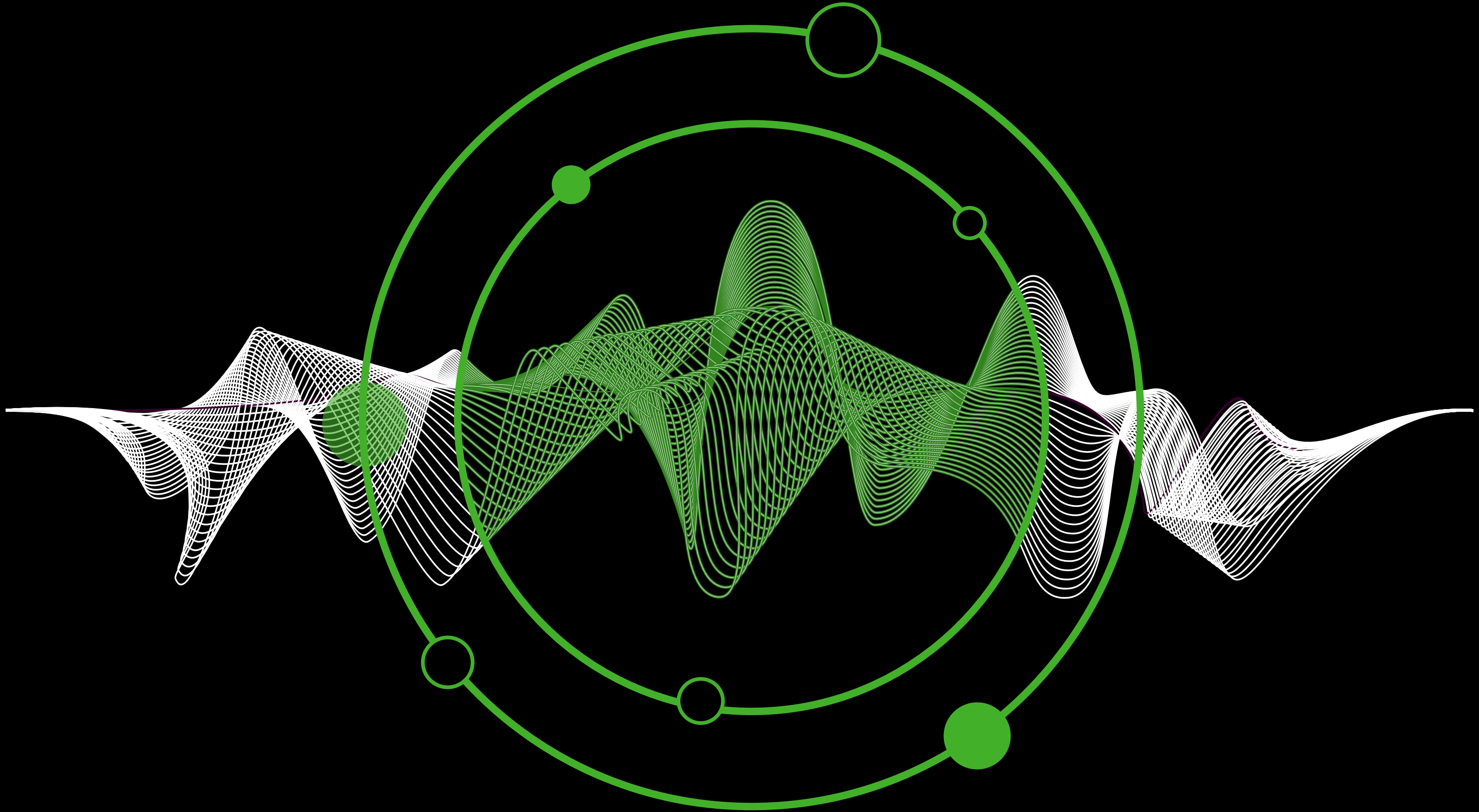
What is it going to take to break cryptography with a quantum computer?

Itan Barmes

Team lead at Deloitte

ENTRUST HID PKI Consortium

Deloitte.

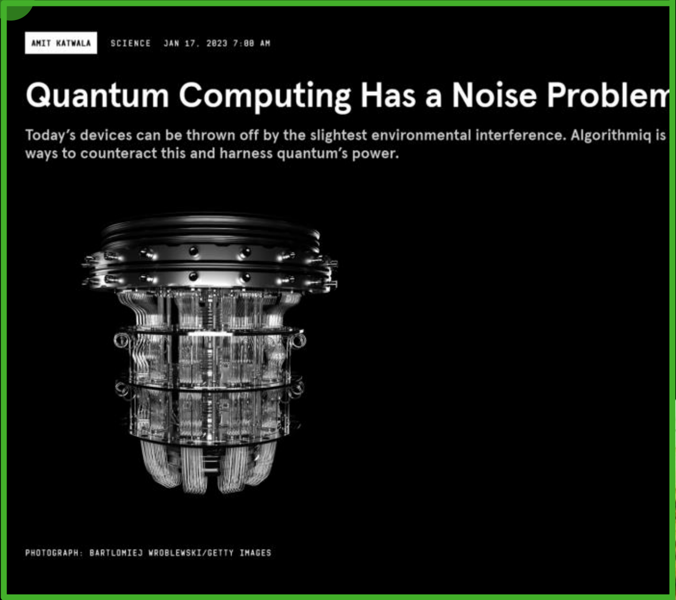


What is it really going to take to break cryptography with a quantum computer?

Itan Barmes, PKIC event, November 2023

What is it really going to take to break cryptography with a quantum computer?

Why is this topic so confusing?

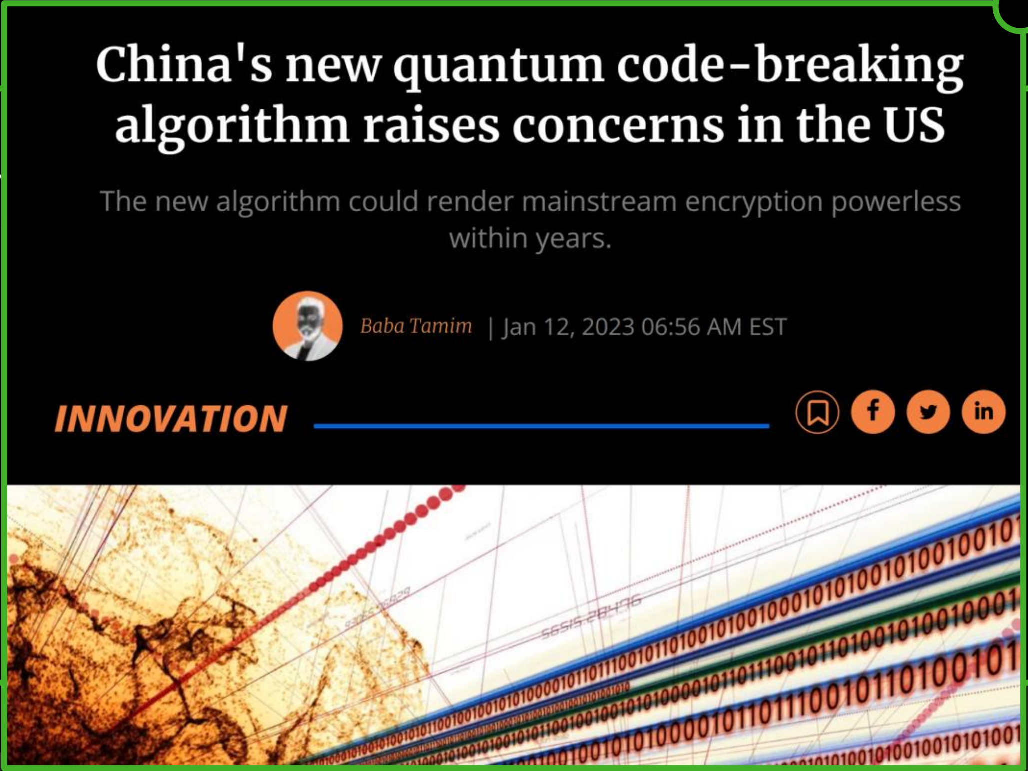


AMIT KATWALA SCIENCE JAN 17, 2023 7:00 AM

Quantum Computing Has a Noise Problem

Today's devices can be thrown off by the slightest environmental interference. Algorithmiq is ways to counteract this and harness quantum's power.

PHOTOGRAPH: BARTLOMIEJ WROBLEWSKI/GETTY IMAGES

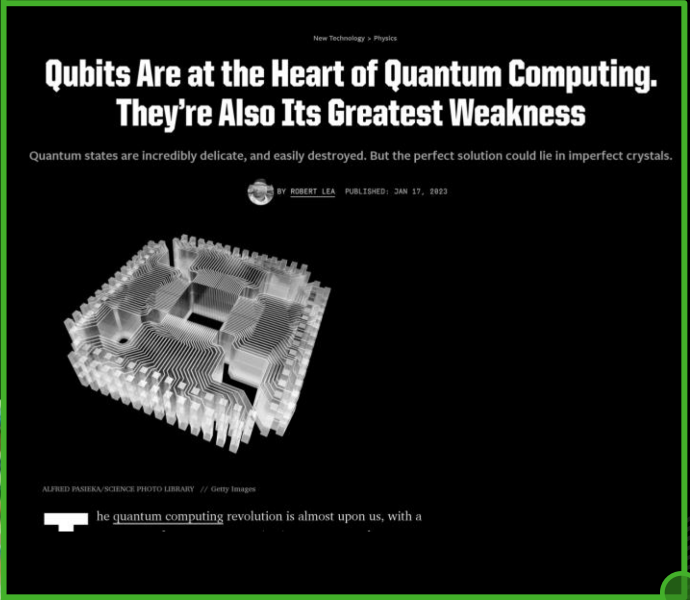


China's new quantum code-breaking algorithm raises concerns in the US

The new algorithm could render mainstream encryption powerless within years.

Baba Tamim | Jan 12, 2023 06:56 AM EST

INNOVATION



New Technology > Physics

Qubits Are at the Heart of Quantum Computing. They're Also Its Greatest Weakness

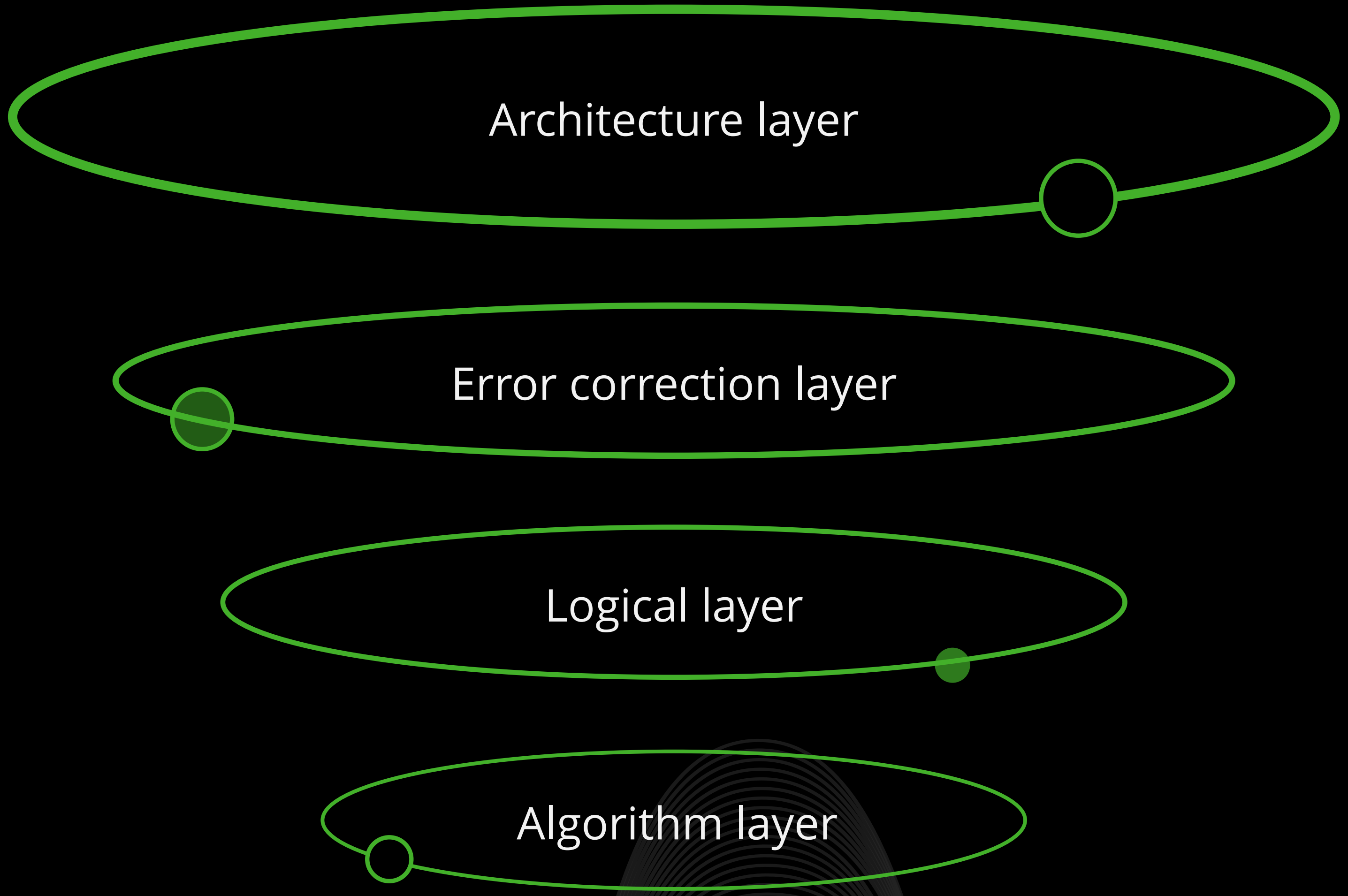
Quantum states are incredibly delicate, and easily destroyed. But the perfect solution could lie in imperfect crystals.

BY ROBERT LEA PUBLISHED: JAN 17, 2023

ALFRED PASIEKA/SCIENCE PHOTO LIBRARY // Getty Images

The quantum computing revolution is almost upon us, with a

Four layers of a quantum algorithm

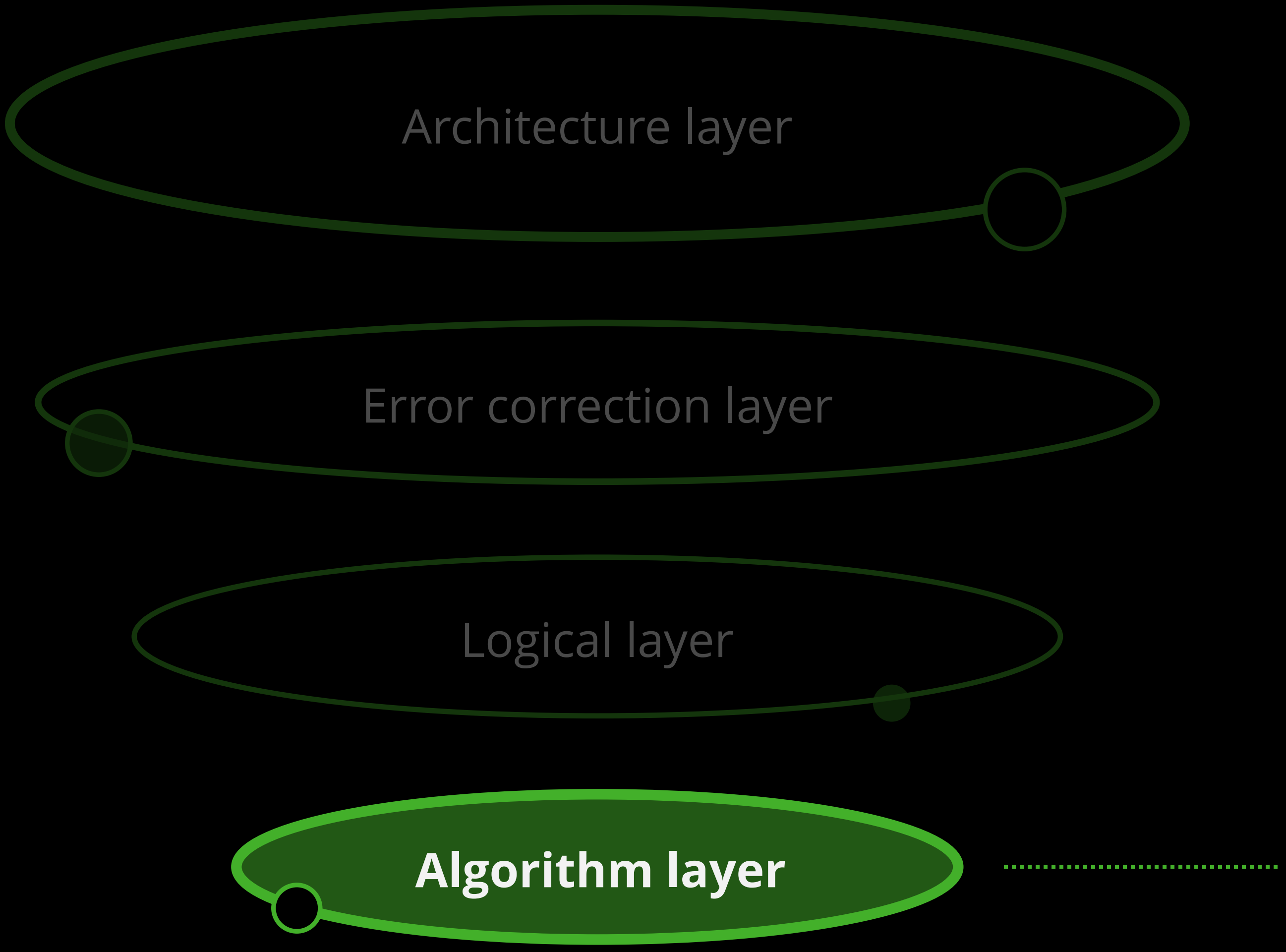


Architecture layer

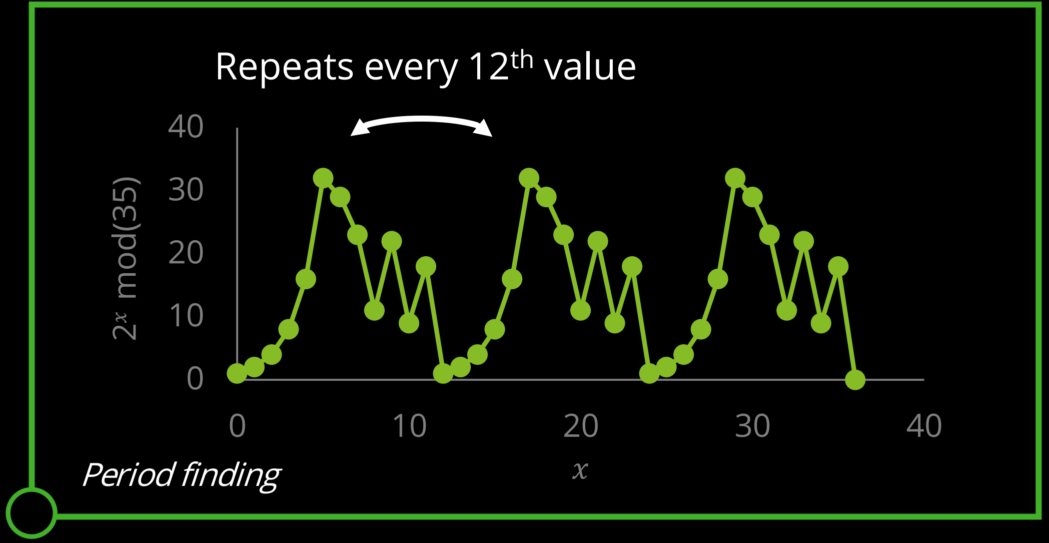
Error correction layer

Logical layer

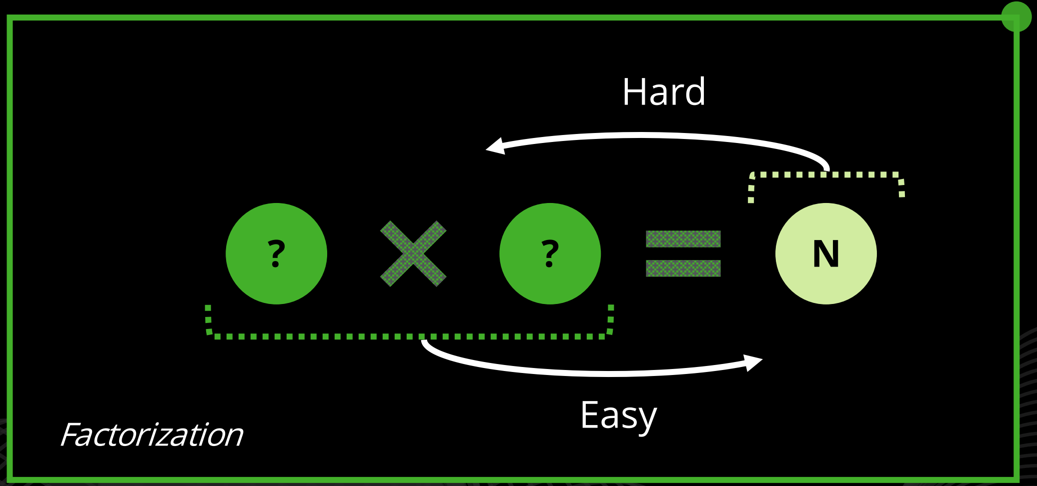
Algorithm layer

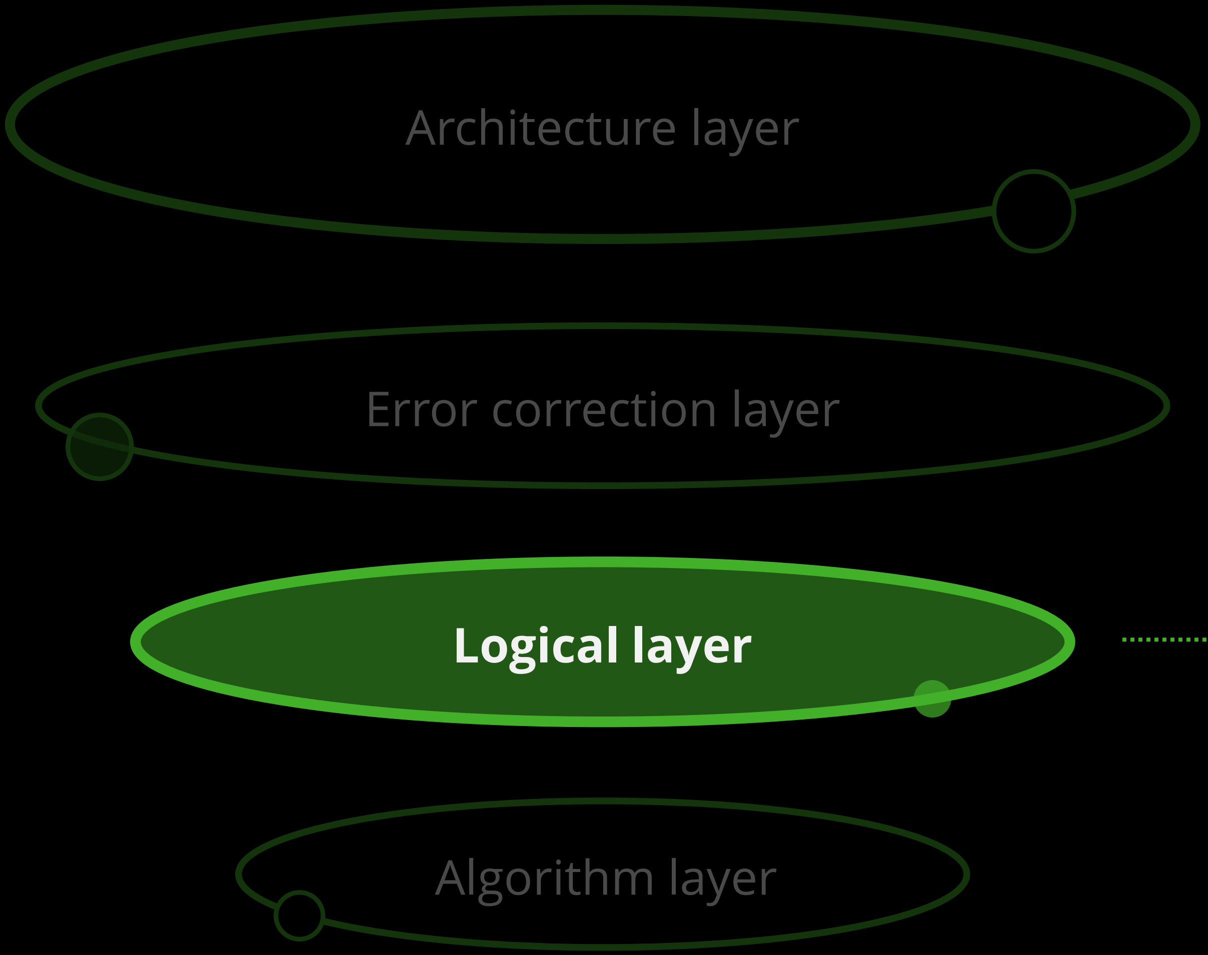


How Shor’s algorithm deals with it



The problem we’re trying to solve



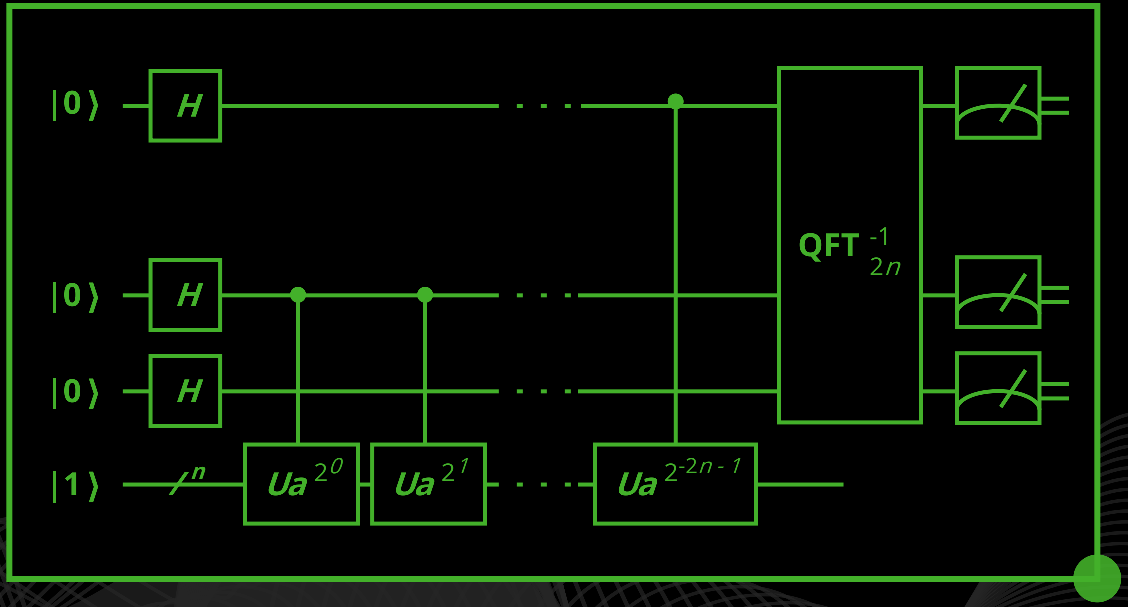


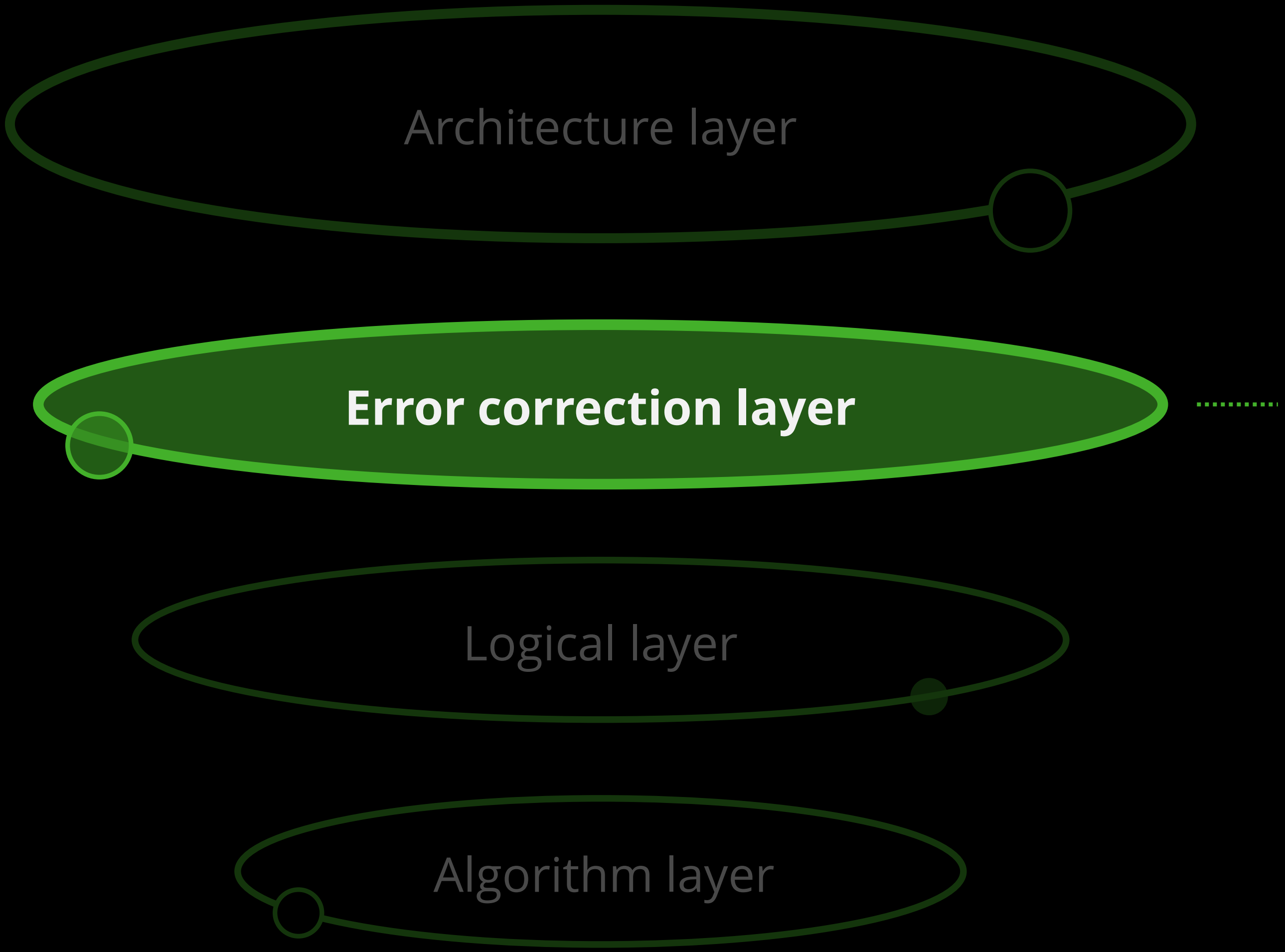
What is the best circuit?

- Minimal number of qubits?
- Low circuit depth (number of sequential operations)?
- Minimal number of specific gates (most expensive)?

Important: number of qubits is not the whole story!

We want to build a circuit we can run





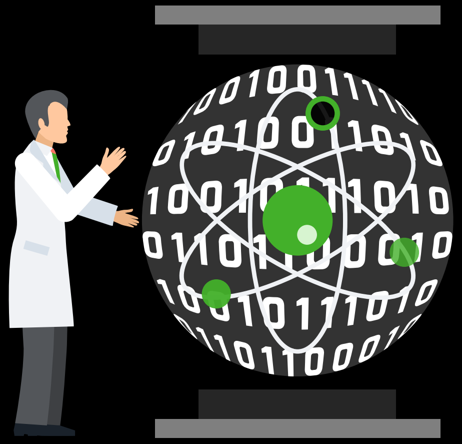
Architecture layer

Error correction layer

Logical layer

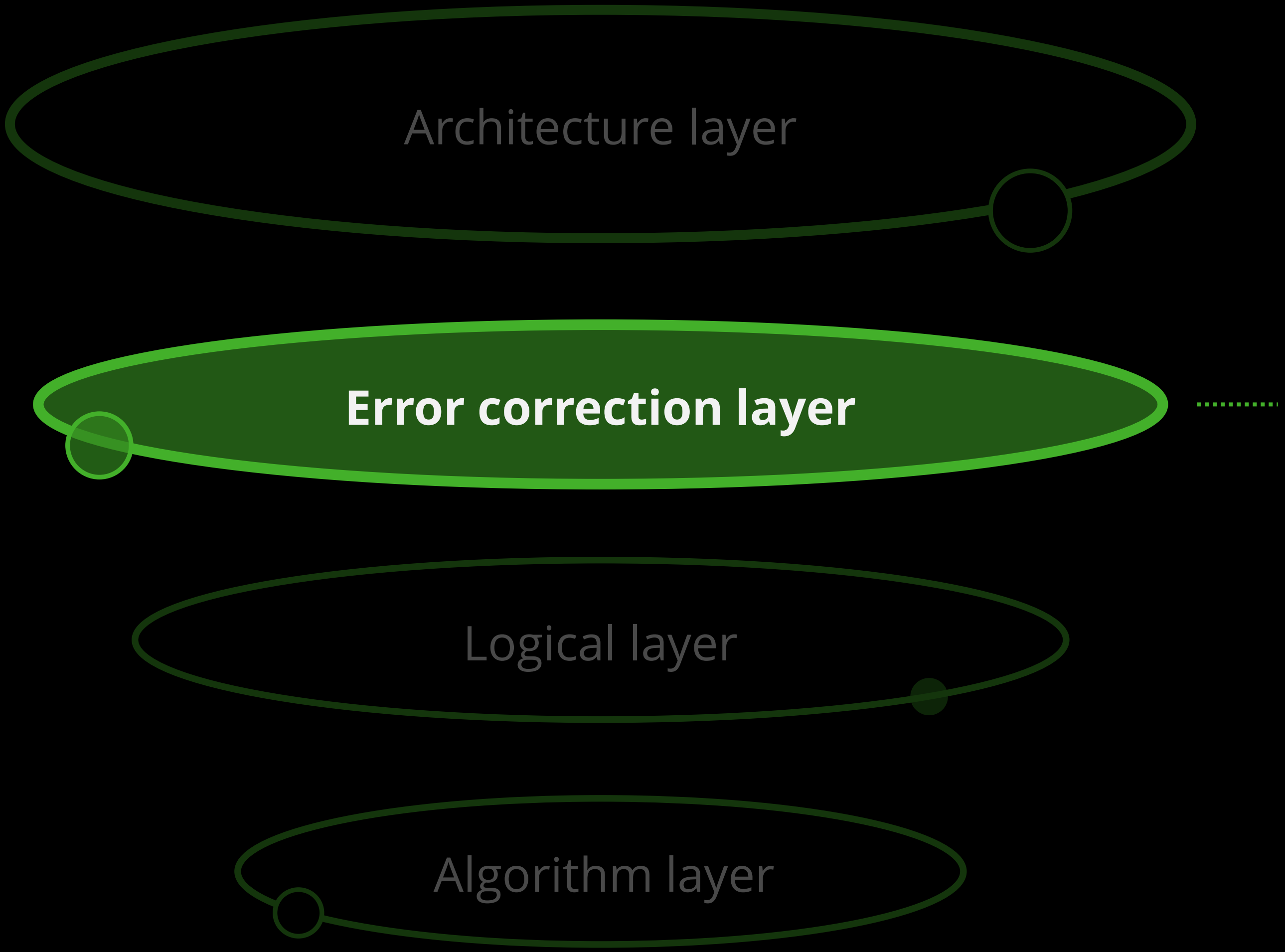
Algorithm layer

Qubits and quantum gates are difficult to realize in the lab!



We need error correction….

But Quantum error correction is really hard



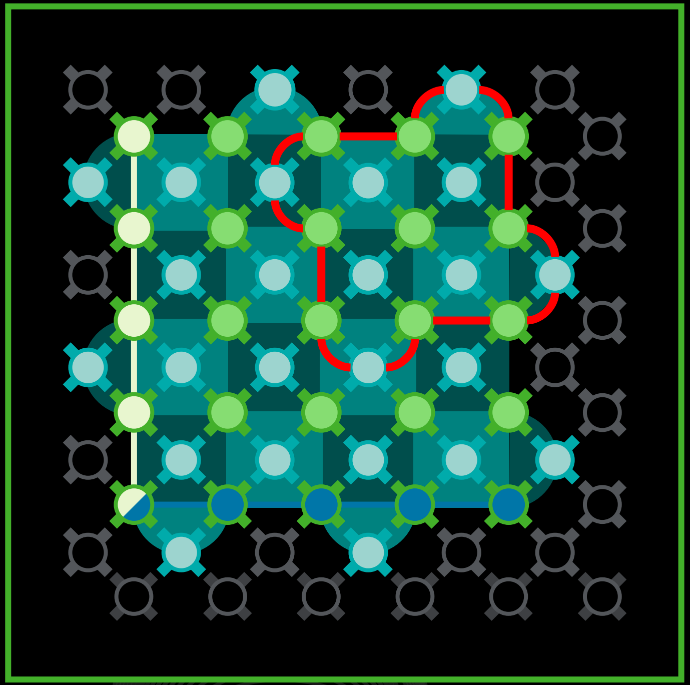
Architecture layer

Error correction layer

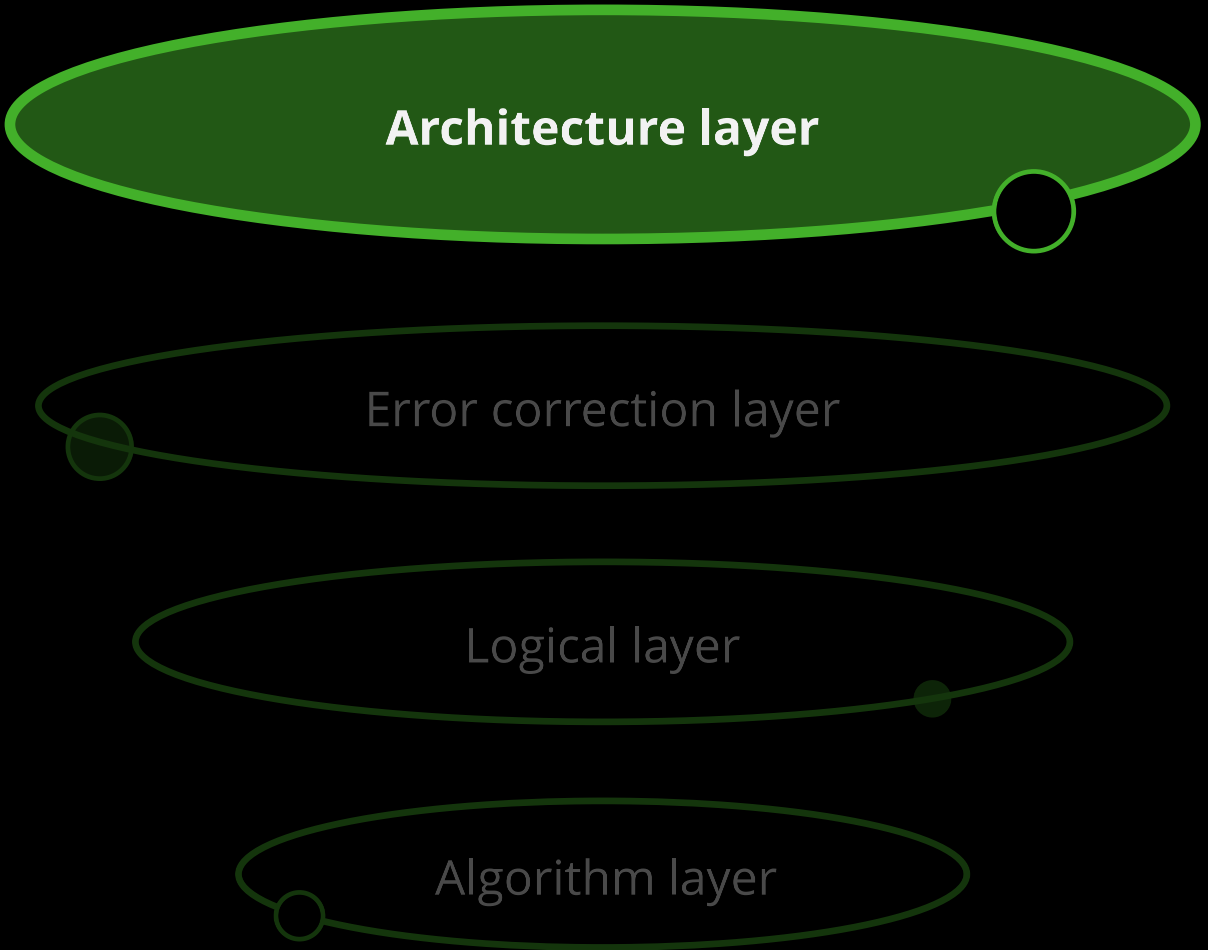
Logical layer

Algorithm layer

- Error correction incurs a large overhead (number of qubits and processing time)
- Estimates of # of physical qubits for each logical qubit vary strongly



Google Sycamore – 72 qubits



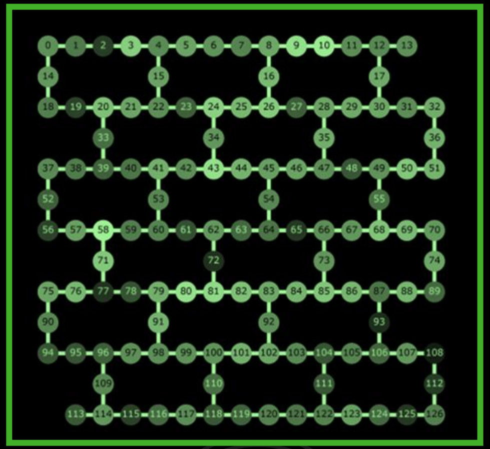
Architecture layer

Error correction layer

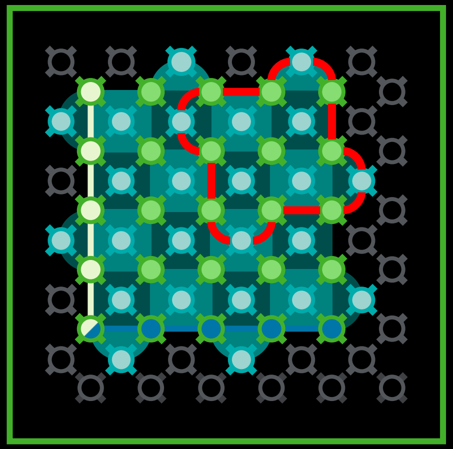
Logical layer

Algorithm layer

- Different qubit types have different tradeoffs
- Some architectures might have a large impact on lowering the resource required, for example novel error correction codes



IBM Eagle – 127 qubits



Google Sycamore – 72 qubits

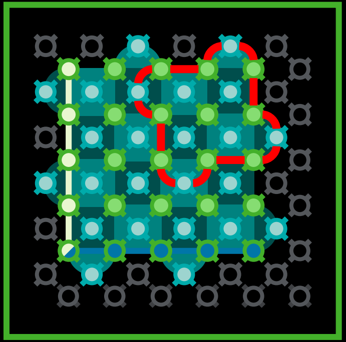
Architecture layer

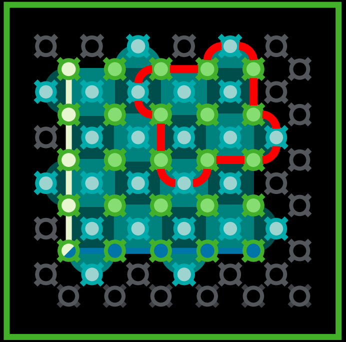
Error correction layer

Logical layer

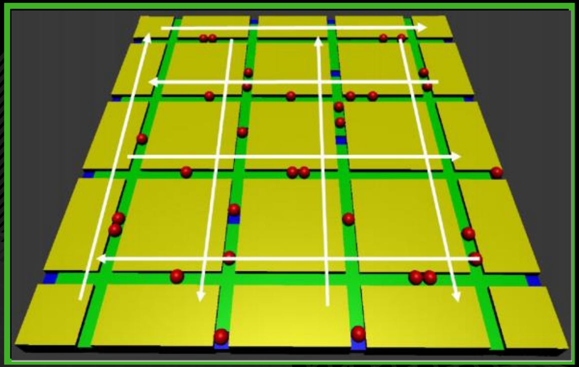
Algorithm layer

- Interconnect

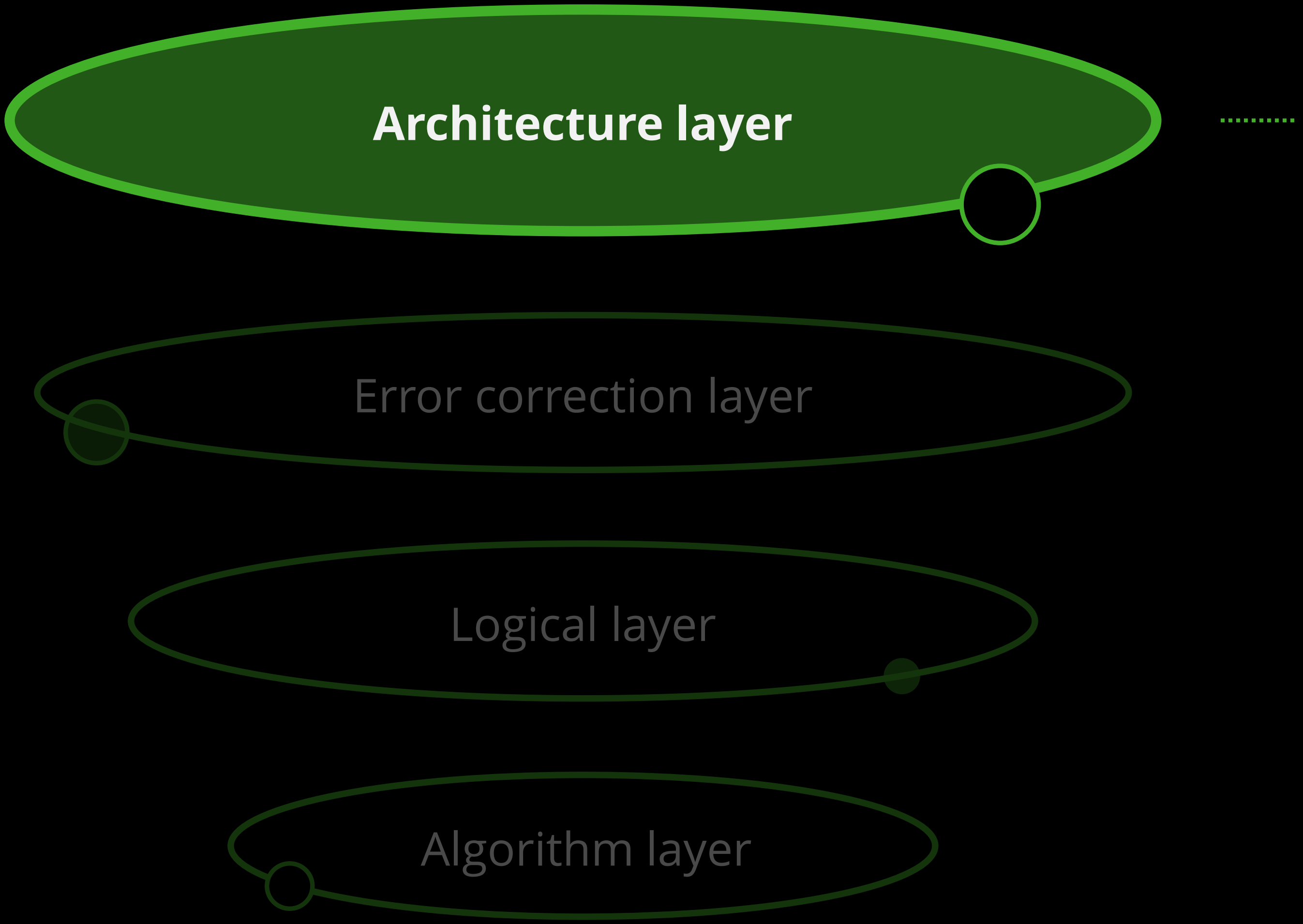




- Shuttling



There are huge differences between types of qubits

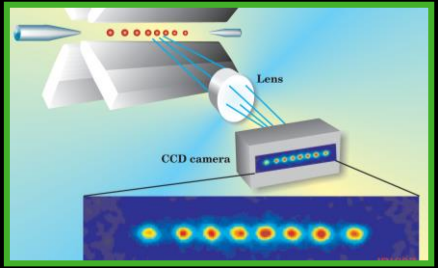


Architecture layer

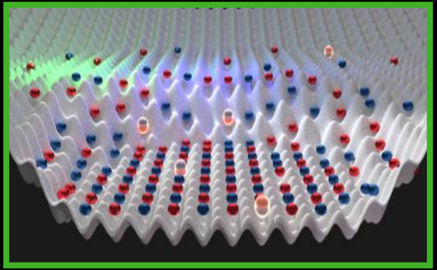
Error correction layer

Logical layer

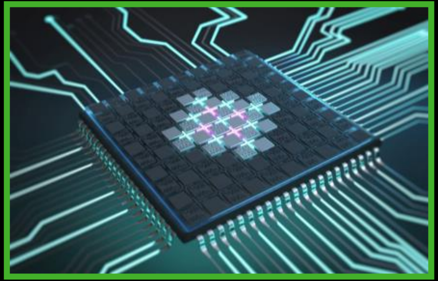
Algorithm layer



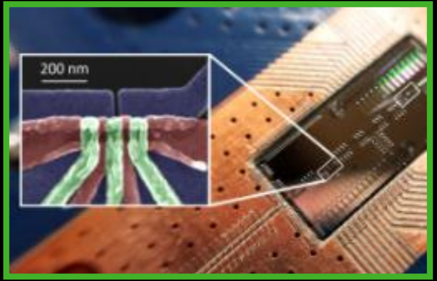
Ion trap



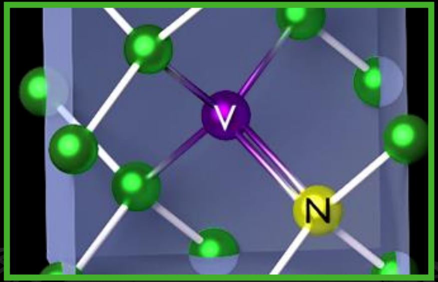
Neutral atoms



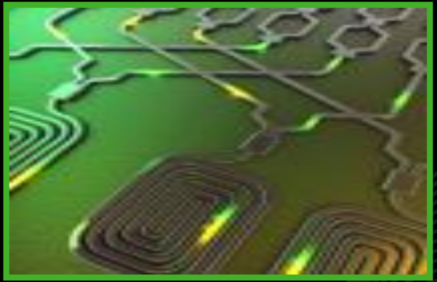
Superconducting



Quantum dot

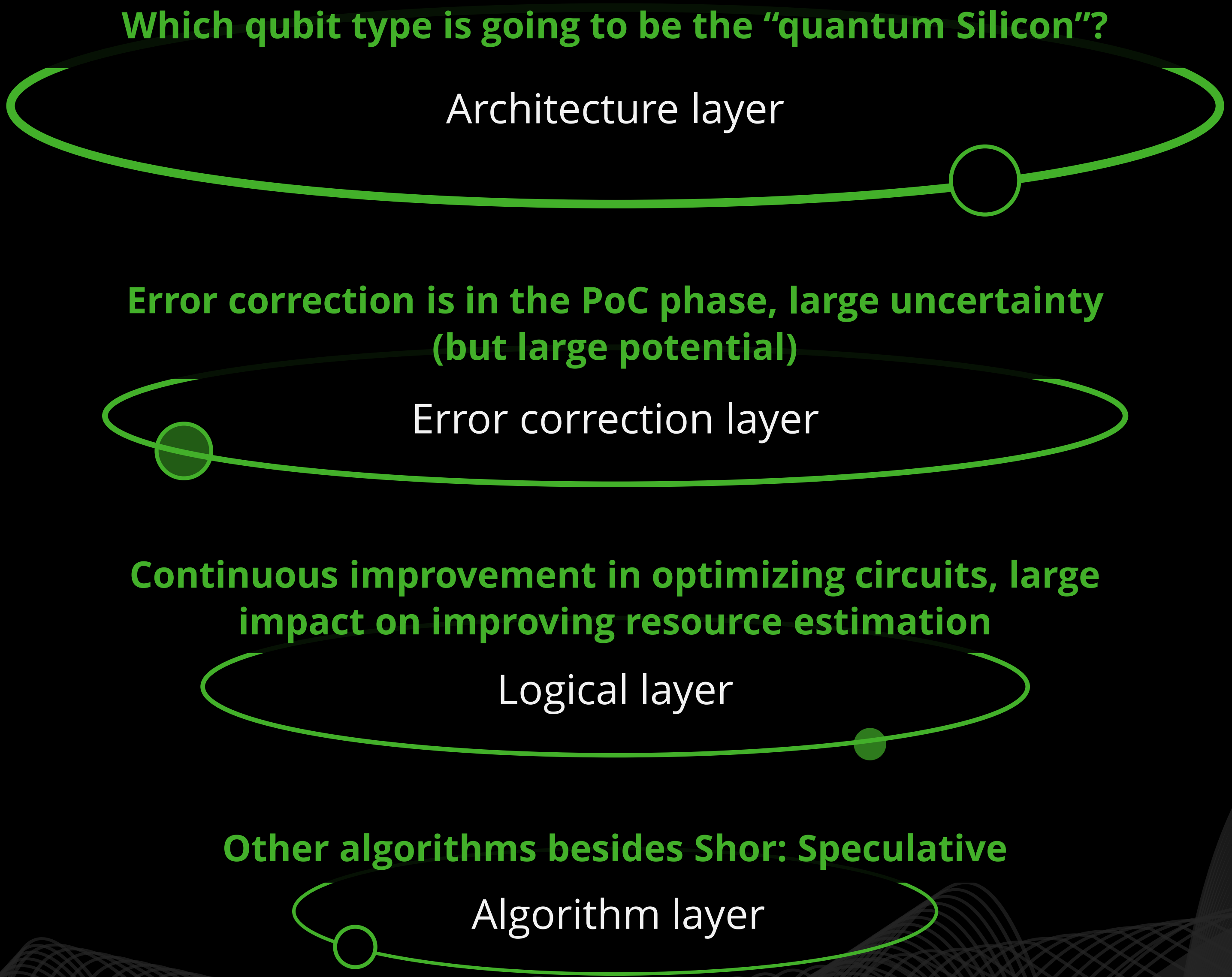


NV center



Photonic qubits

What can we expect at each layer?



Which qubit type is going to be the "quantum Silicon"?

Architecture layer

Error correction is in the PoC phase, large uncertainty (but large potential)

Error correction layer

Continuous improvement in optimizing circuits, large impact on improving resource estimation

Logical layer

Other algorithms besides Shor: Speculative

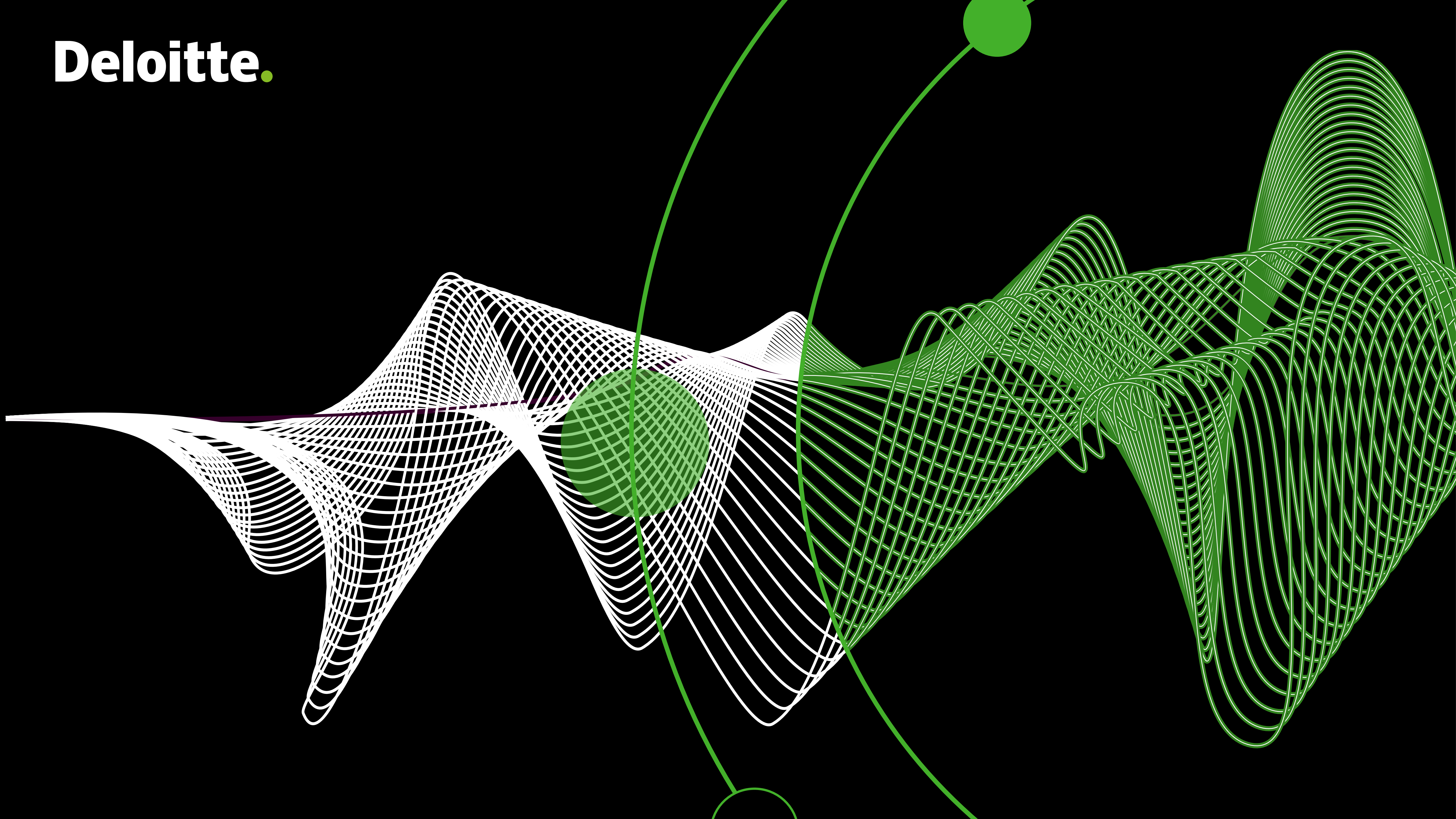
Algorithm layer

The bottom line is

We should not fixate on the number of qubits as a measure of progress

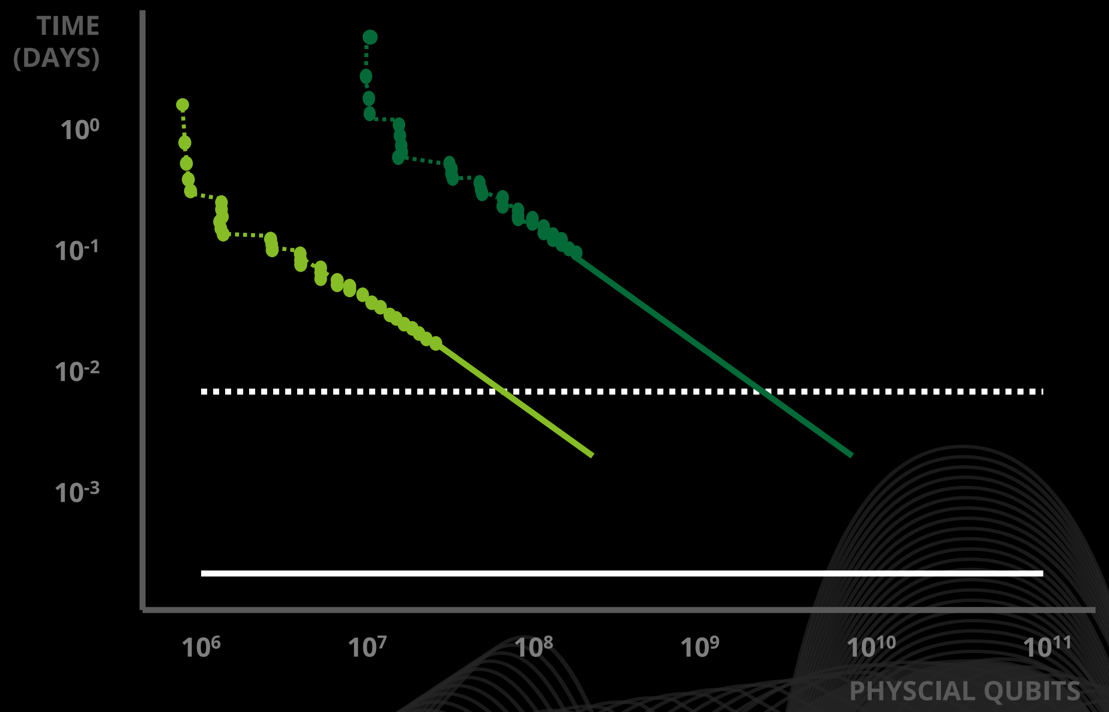
We are just too early for having enough confidence in extrapolating the progress

Deloitte.



Additional slides

Bringing it all together



Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

01 COMMUNIQUE

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia