Quantum AI

When ECC and RSA Break: Urgency of Migrating to Post-Quantum Cryptography

based on research published in *PRX Quantum*:
"Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations"

doi.org/10.1103/j3xf-bw18

Ryan Babbush, **Adam Zalcman**, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi (Berkeley), Justin Drake (Ethereum) and Dan Boneh (Stanford)

3 September 2026
Global Digital Collaboration Conference 2026
Geneva, Switzerland

Quantum AI

A significant portion of currently deployed public-key cryptography is based on the assumption that the **elliptic curve discrete logarithm problem** (ECDLP) is hard to solve.

However, ECDLP can be solved easily using Shor's algorithm on a **cryptographically relevant quantum computer** (CRQC).

ECDLP-based cryptography is widespread

- Hardware Root of Trust
- Electronic Passports
- Transport Layer Security
- Secure Boot
- Multi-factor Authentication
- Internet of Things
- Encrypted Messaging
- Secure Shell
- Blockchains

Structure of blockchain economy

ECDLP is hard to solve

random function is hard to invert

hardness assumptions

Structure of blockchain economy

ECDSA

Schnorr signatures

SHA-256

Groth16

cryptographic schemes

ECDLP is hard to solve

random function is hard to invert

hardness assumptions

Quantum AI

Structure of blockchain economy

PoW mining | Taproot | MWEB | DAS — blockchain features

ECDSA | Schnorr signatures | SHA-256 | Groth16 — cryptographic schemes

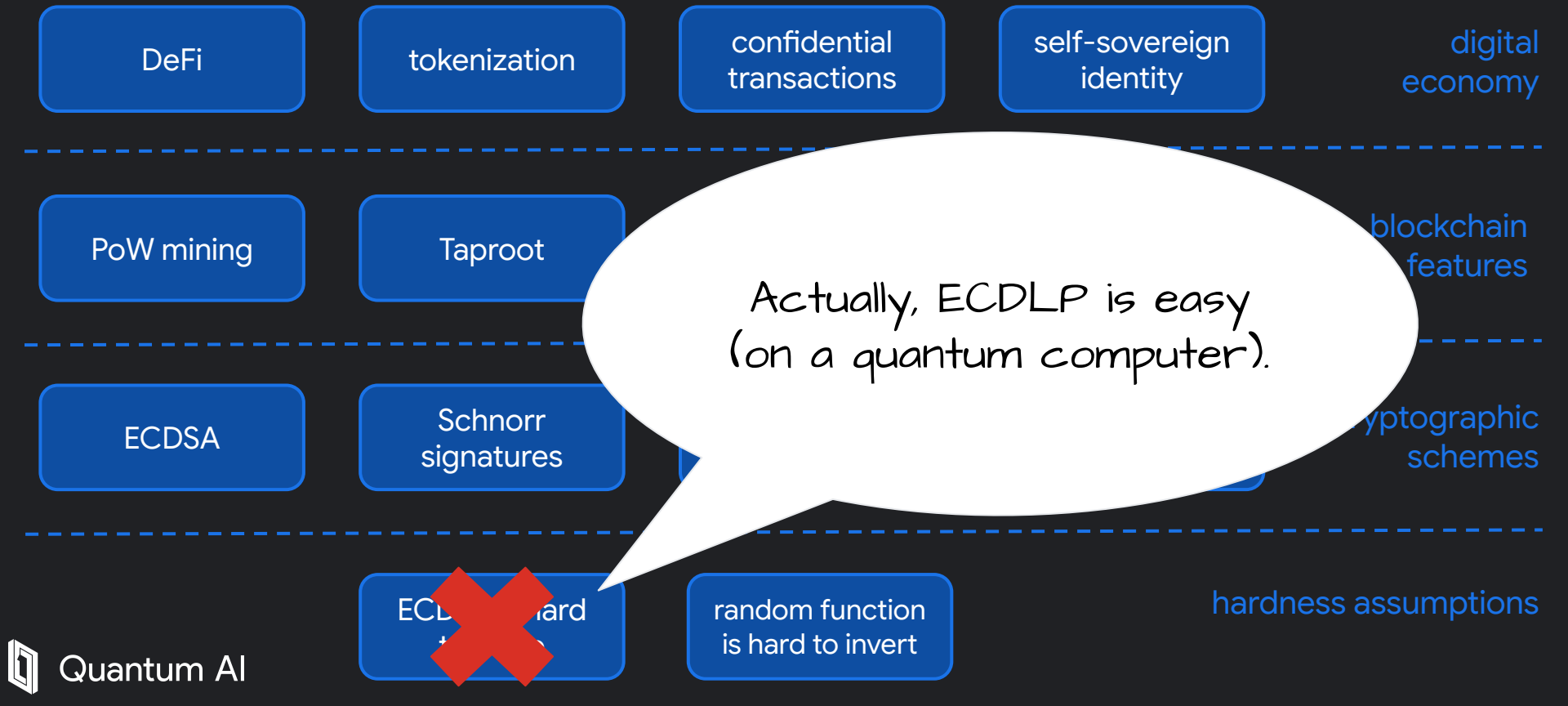
ECDLP is hard to solve | random function is hard to invert — hardness assumptions

Quantum AI

Structure of blockchain economy

DeFi	tokenization	confidential transactions	self-sovereign identity	digital economy
PoW mining	Taproot	MWEB	DAS	blockchain features
ECDSA	Schnorr signatures	SHA-256	Groth16	cryptographic schemes
	ECDLP is hard to solve	random function is hard to invert		hardness assumptions

Blockchain economy rests on a **false** hardness assumption



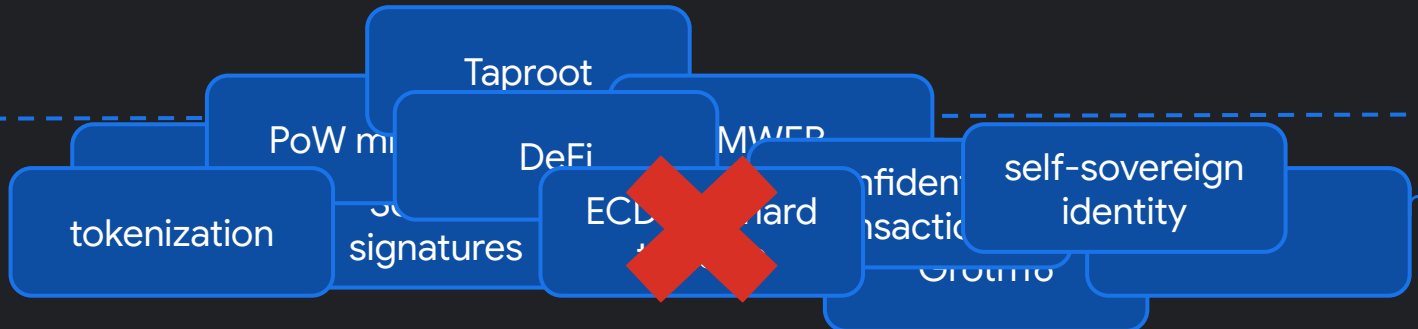
Quantum AI

Blockchain economy rests on a **false** hardness assumption

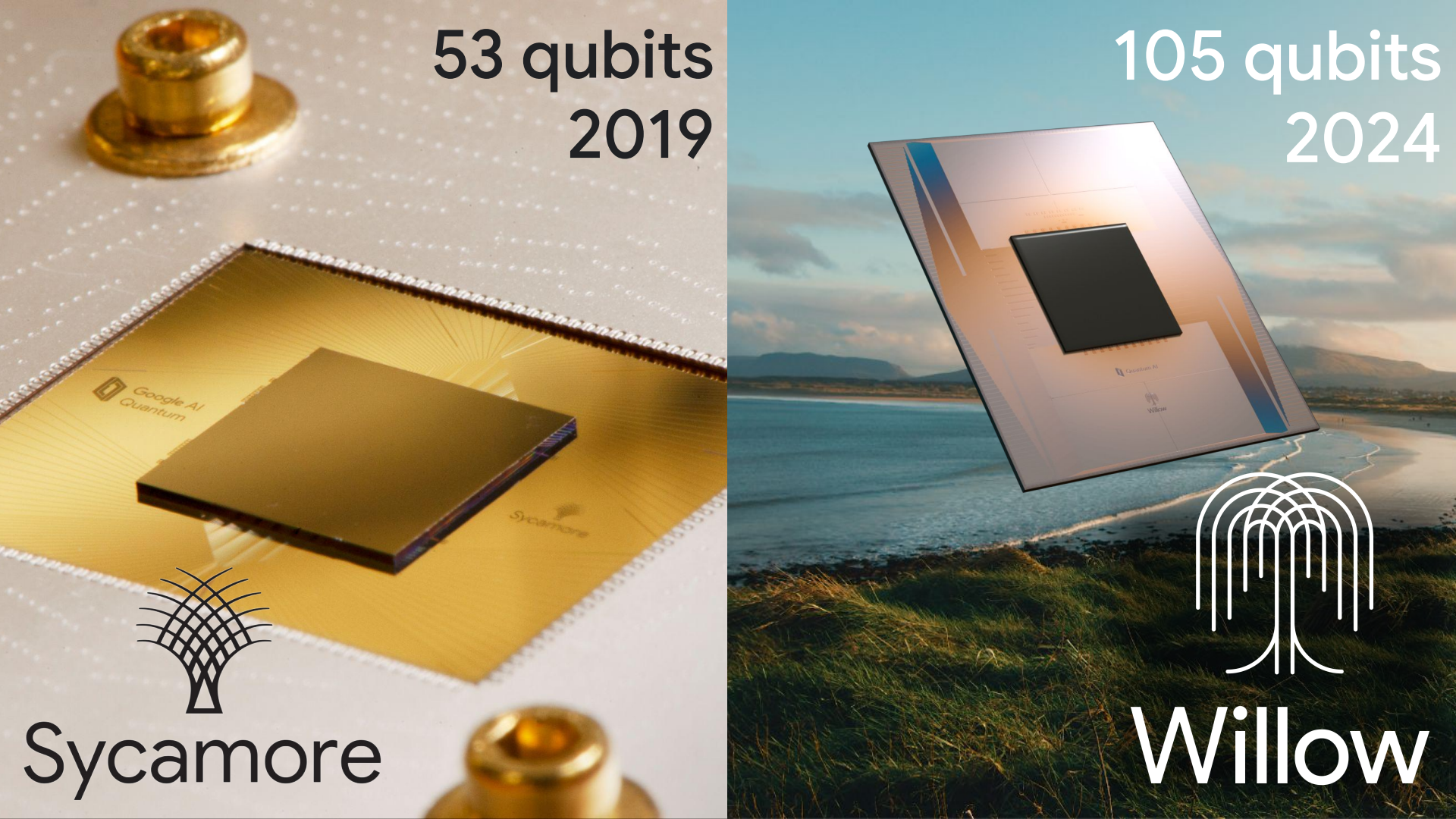
digital economy

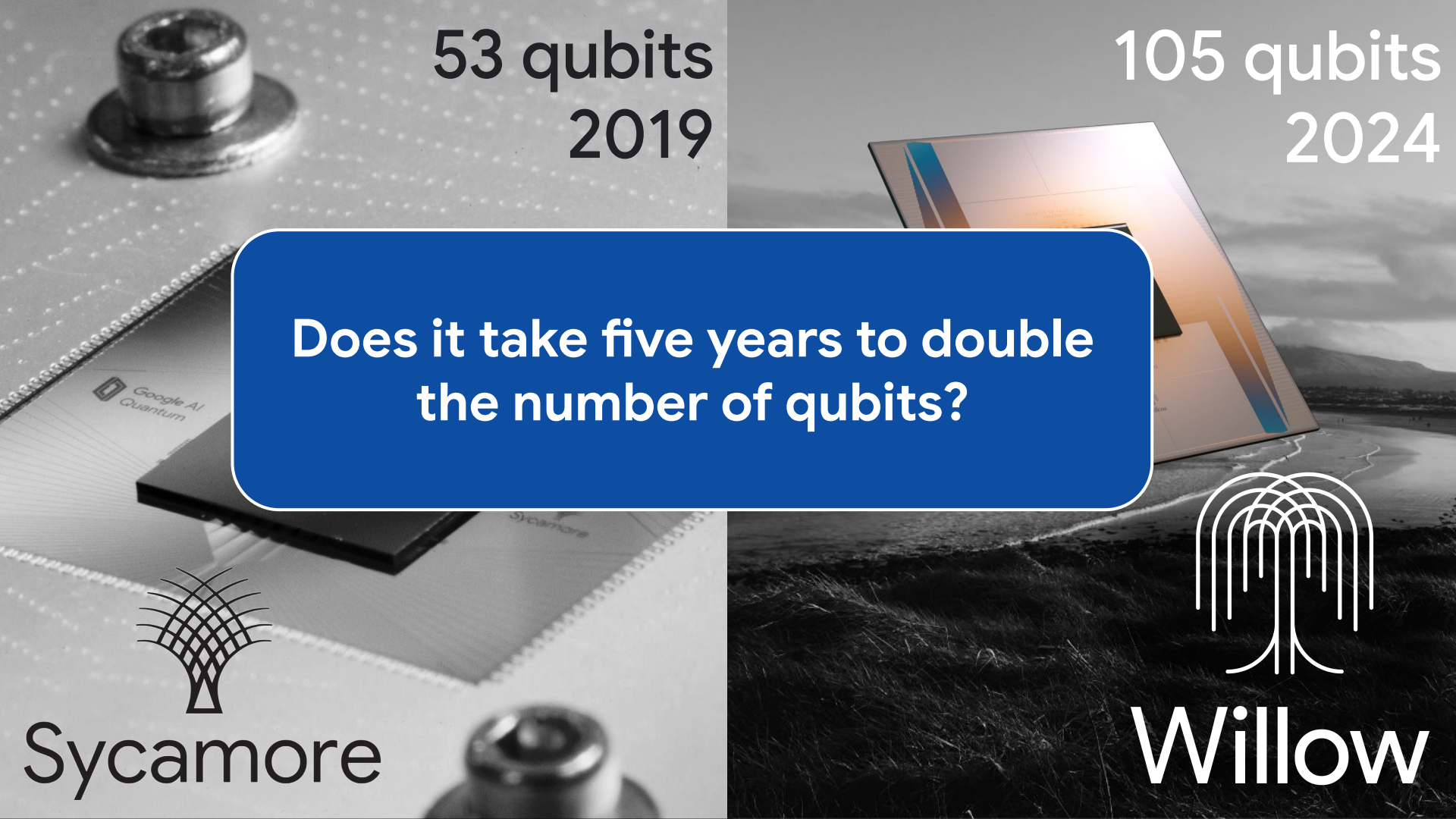
blockchain features

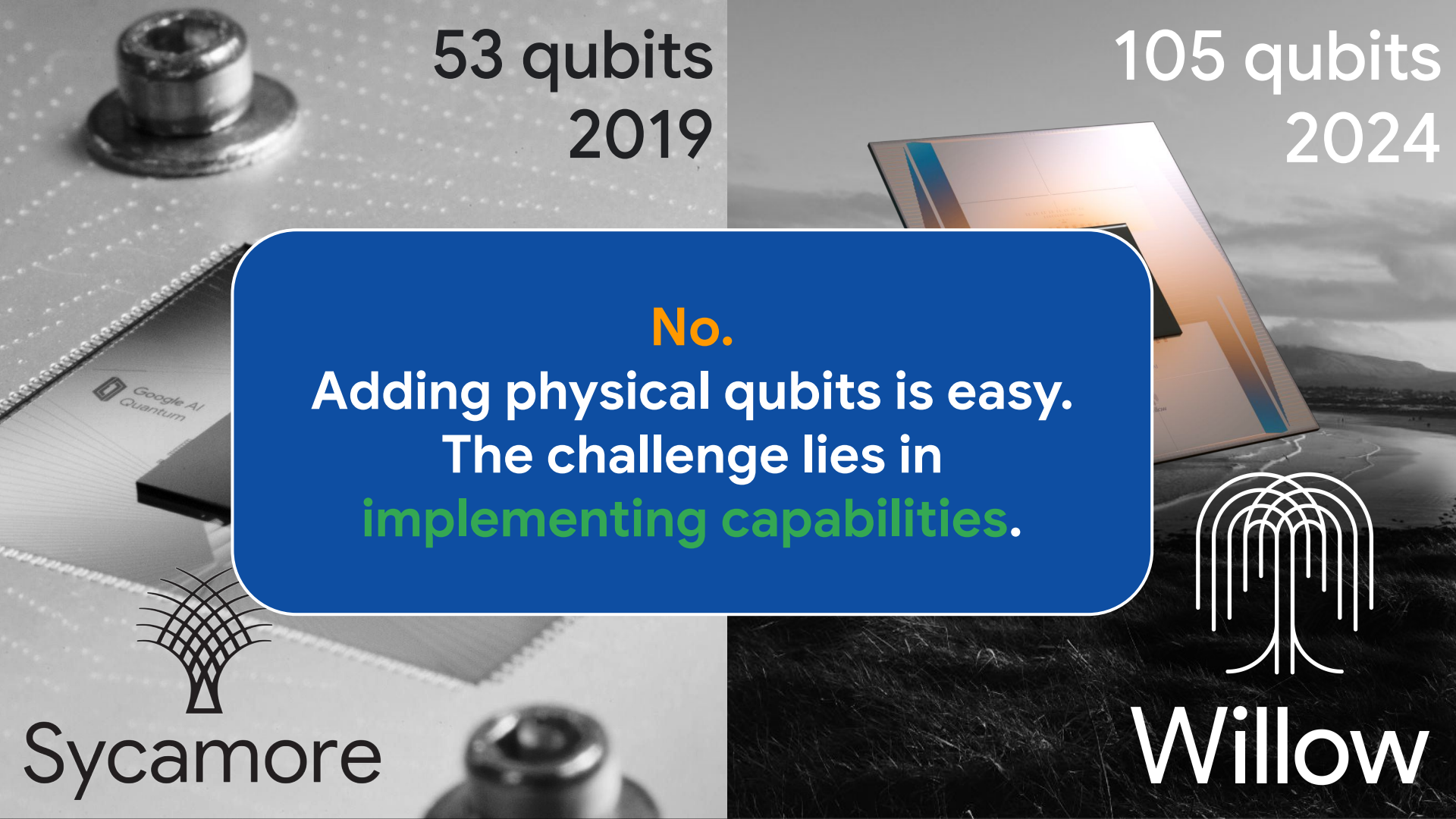
cryptographic schemes



hardness assumption


53 qubits
2019
Google AI Quantum
Sycamore
Sycamore
105 qubits
2024
Willow


53 qubits
2019
105 qubits
2024
Does it take five years to double the number of qubits?
Google AI Quantum
Sycamore
Sycamore
Willow


53 qubits
2019
105 qubits
2024
No.
Adding physical qubits is easy.
The challenge lies in
implementing capabilities.
Google AI Quantum
Sycamore
Willow


53 qubits
2019
105 qubits
2024
Capabilities introduce
performance discontinuities.
Google AI Quantum
Sycamore
Sycamore
Willow

Example 1: Quantum error correction

Before: Quantum information in a superconducting circuit survives for ~0.0001s

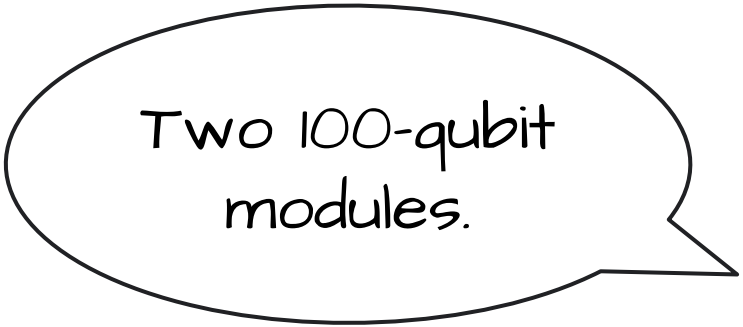
Example 1: Quantum error correction

$$\varepsilon_d \propto \left(\frac{p}{p_{\text{thr}}}\right)^{(d+1)/2}$$

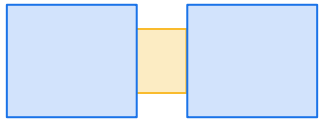
Before: Quantum information in a superconducting circuit survives for ~0.0001s

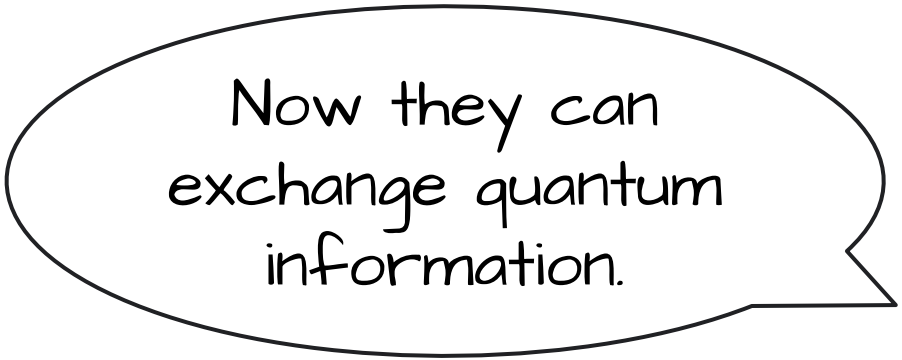
After: Quantum information in a superconducting circuit survives for essentially however long you wish

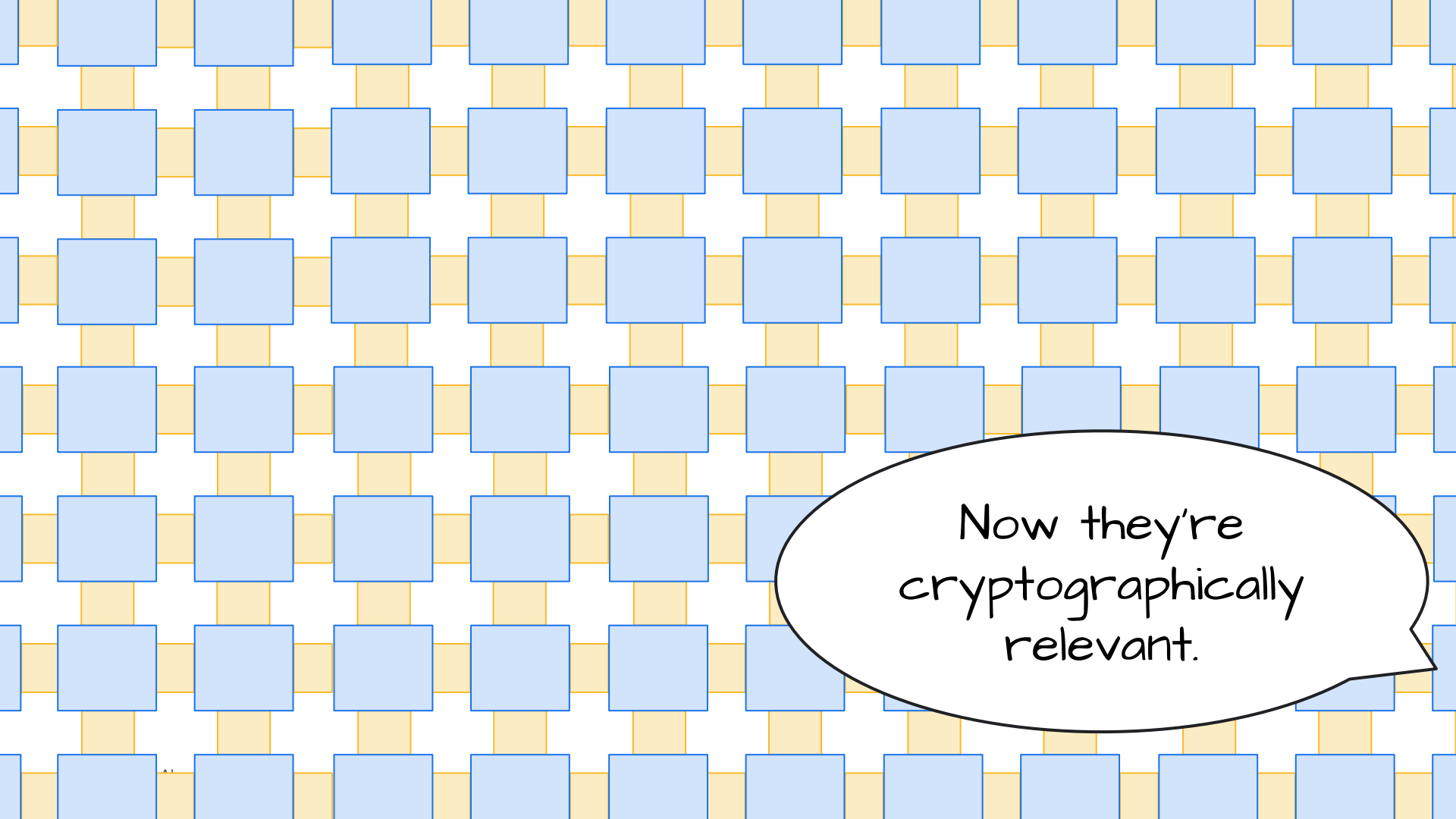
Example 2: Copy-paste modules

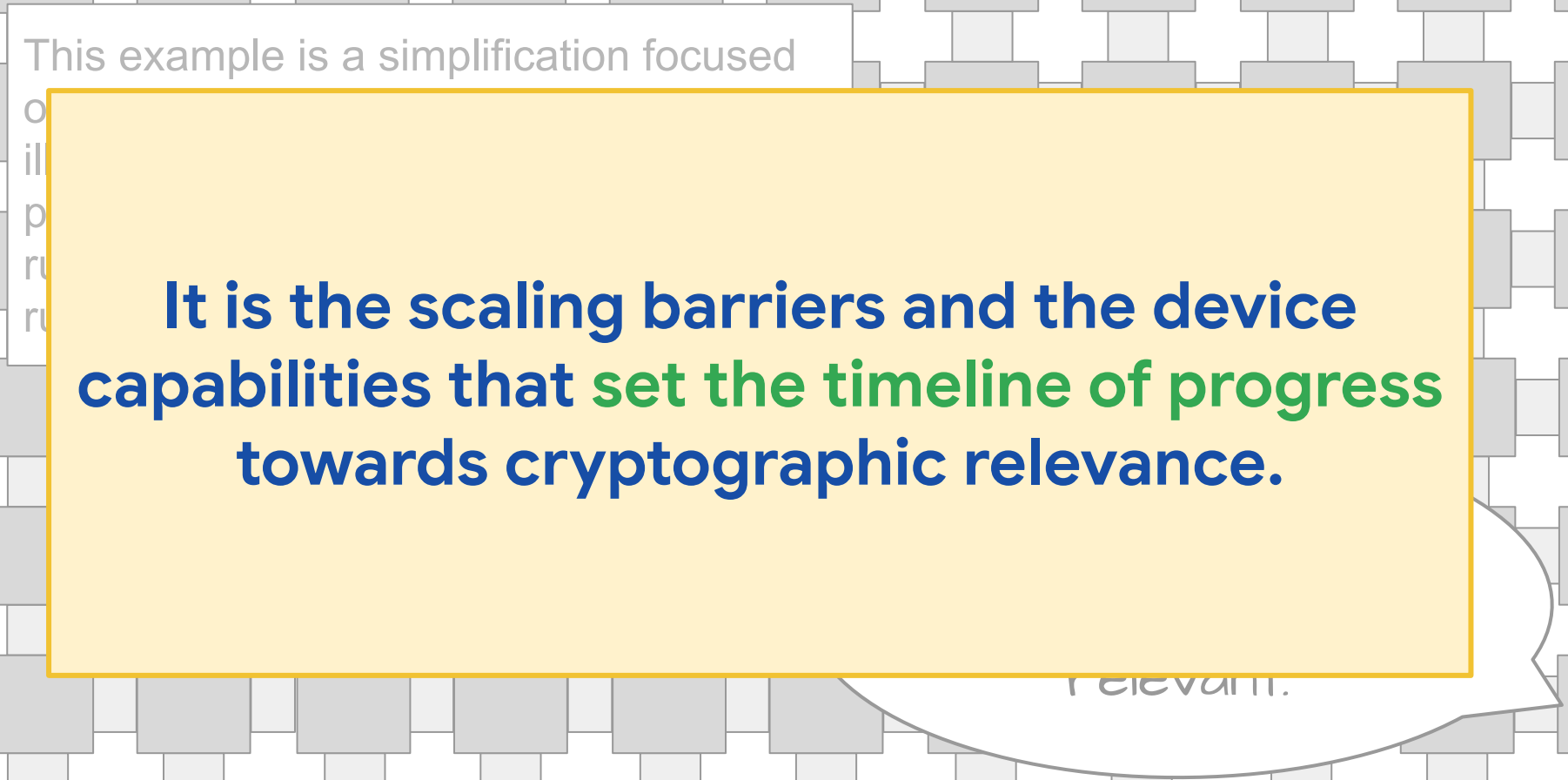


Example 2: Copy-paste modules

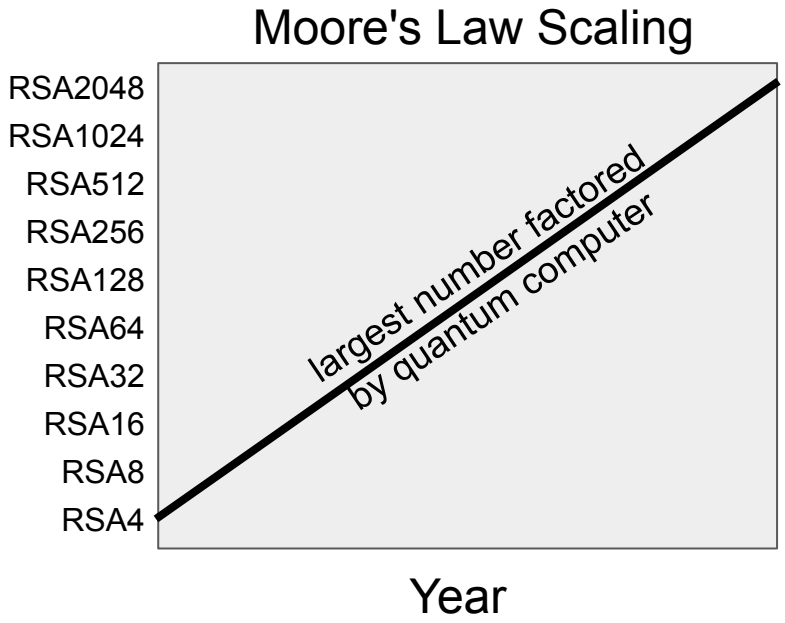




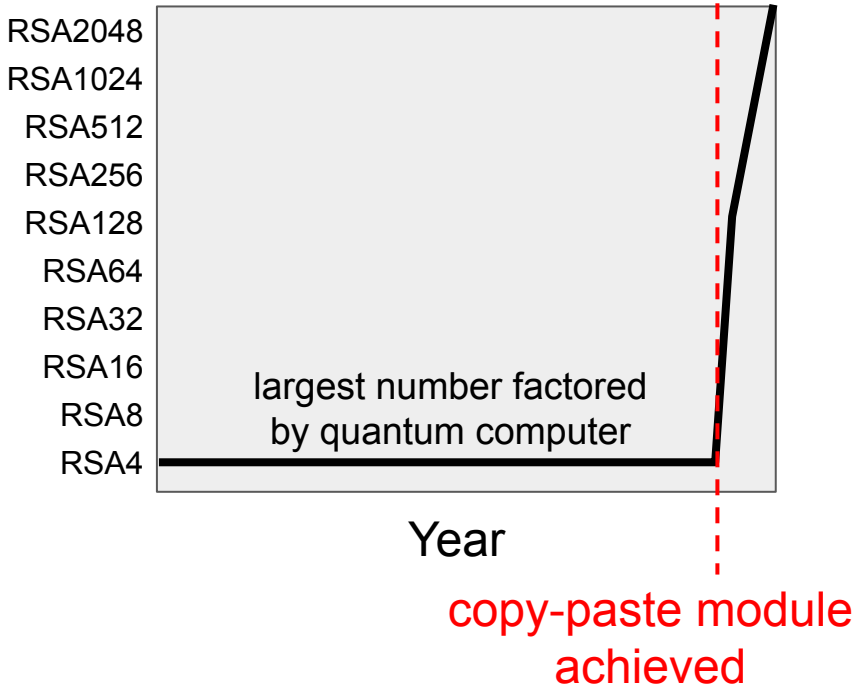

Now they're cryptographically relevant.


This example is a simplification focused
It is the scaling barriers and the device capabilities that set the timeline of progress towards cryptographic relevance.

What I think many people think will happen

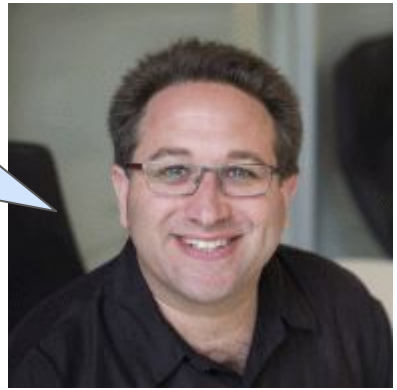


What I think will happen



Beware expecting gradual progress

Once you understand quantum fault-tolerance, asking "*so when are you going to factor 35 with Shor's algorithm?*" becomes sort of like asking the **Manhattan Project** physicists in 1943, "*so when are you going to produce **at least a small nuclear explosion**?*"



https://scottaaronson.blog/?p=9665#comment-2029013

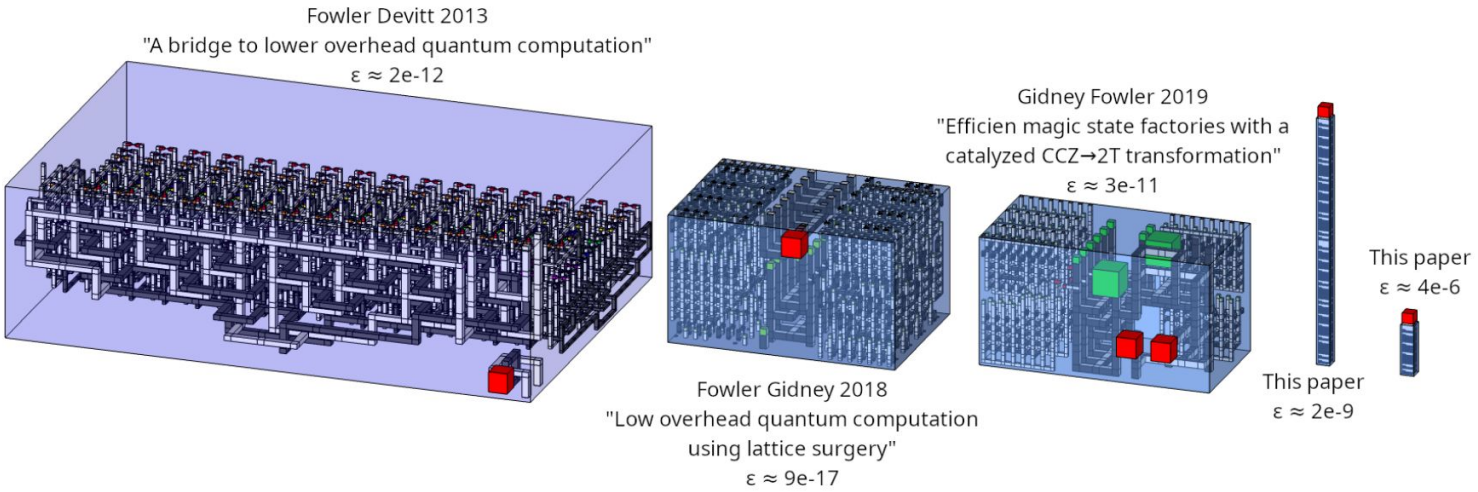
Progress in quantum computing hardware is only one part of the picture.

Another is progress in quantum error correction and compiling.

Progress in compiling is bringing the finish line closer

2012 → 2024

Computational volume required for magic state creation



C. Gidney et al, arXiv:2409.17595 (2024)

Quantum attacks by onchain consequences

Security property breached	Example
asset ownership	transaction forgery in Bitcoin
consensus	deep blockchain reorganization in Ethereum
confidentiality	attacks on unlinkability of diversified addresses in Zcash
monetary integrity	creation of new coin in Mimblewimble sidechain of Litecoin
solvency	peg collapse due to illegitimate stablecoin redemptions
data availability	forging a data availability sampling proof in Ethereum
governance	vote forgery in Cardano
…	…

Quantum attacks by capability required

Attack mode	Operational demands on CRQC
on-spend	requires access to a **fast-clock** CRQC **during attack**
at-rest	requires access to any CRQC **during attack**
on-setup	requires knowledge of a **universal classical exploit** produced in a **one-off** quantum computation **before attacks**

Migrate to post-quantum cryptography (PQC)

DeFi	tokenization	confidential transactions	self-sovereign identity	digital economy
PoW mining	Taproot	MWEB	DAS	blockchain features
ECDSA	Schnorr signatures	SHA-256	Groth16	cryptographic schemes
	ECDLP is hard to solve	random function is hard to invert		hardness assumptions

Quantum AI

Migrate to post-quantum cryptography (PQC)

DeFi	tokenization	confidential transactions	self-sovereign identity	digital economy
PoW mining	Taproot	MWEB	DAS	blockchain features
ECDSA	Schnorr signatures	SHA-256	Groth16	cryptographic schemes
	ECDLP is hard to solve	random function is hard to invert		hardness assumptions

Quantum AI

Migrate to post-quantum cryptography (PQC)

DeFi	tokenization	confidential transactions	self-sovereign identity	digital economy
PoW mining	Quantumroot	WOTS	`falcon_verify`	blockchain features
ML-DSA	FALCON	SHA-256	STARKs	cryptographic schemes
	LWE is hard to solve	random function is hard to invert		hardness assumptions

Quantum AI

Thank you!

PRX Quantum **7**, 031001 – **Published 21 August, 2026**
doi.org/10.1103/j3xf-bw18

Ryan Babbush

Adam Zalcman

Craig Gidney

Michael Broughton

Tanuj Khattar

Hartmut Neven

Quantum AI

Thiago Bergamaschi
(Google / UC Berkeley)

Justin Drake
(Ethereum Foundation)

Dan Boneh
(Stanford University)