EVM

www.quantumevm.com

Quantum Computing vs Web3 Cryptography

Risks, Challenges and Opportunities

Quantum Technology Market Map – Quantum Computers

NON-EXHAUSTIVE, NO ORDER, EXCLUDES LABS

THE QUANTUM INSIDER

Neural Atoms

- atom computing
- QuEra Computing Inc.
- PASQAL
- Infleqtion
- AQUARK TECHNOLOGIES
- planqc

NV Diamond

- QUANTUM BRILLIANCE
- SaxonQ
- XEED

Electrons on Helium

- EeroQ

Cavity QED

- NanoQT

Carbon Nanotubes

- C12

Silicon

- diraq
- equal1
- intel
- photonic
- QUANTUM MOTION
- quobly
- SemiQon
- Silicon Quantum Computing
- HITACHI Inspire the Next

Topological Qubits

- QUCOHERENT
- Microsoft

Quantum Annealers

- D-Wave
- QILIMANJARO
- NEC
- Tokyo Quantum Computing

Superconducting

- IQM
- ALICE & BOB
- IBM
- Google Quantum AI
- FUJITSU
- OQC
- QW QUANTWARE
- 本源量子
- Anyon Technologies
- D-Wave The Quantum Computing Company
- RIKEN
- ATLANTIC QUANTUM
- aws
- rigetti
- SPINQ 量旋科技
- qci

Trapped Ion

- CRYSTAL QUANTUM COMPUTING
- QUANTINUUM
- Universal Quantum
- AQT
- oxford ionics
- eleQtron
- ROSATOM
- Quantum Art
- QUDOOR 启科量子
- FOXCONN
- HYQ
- IONQ

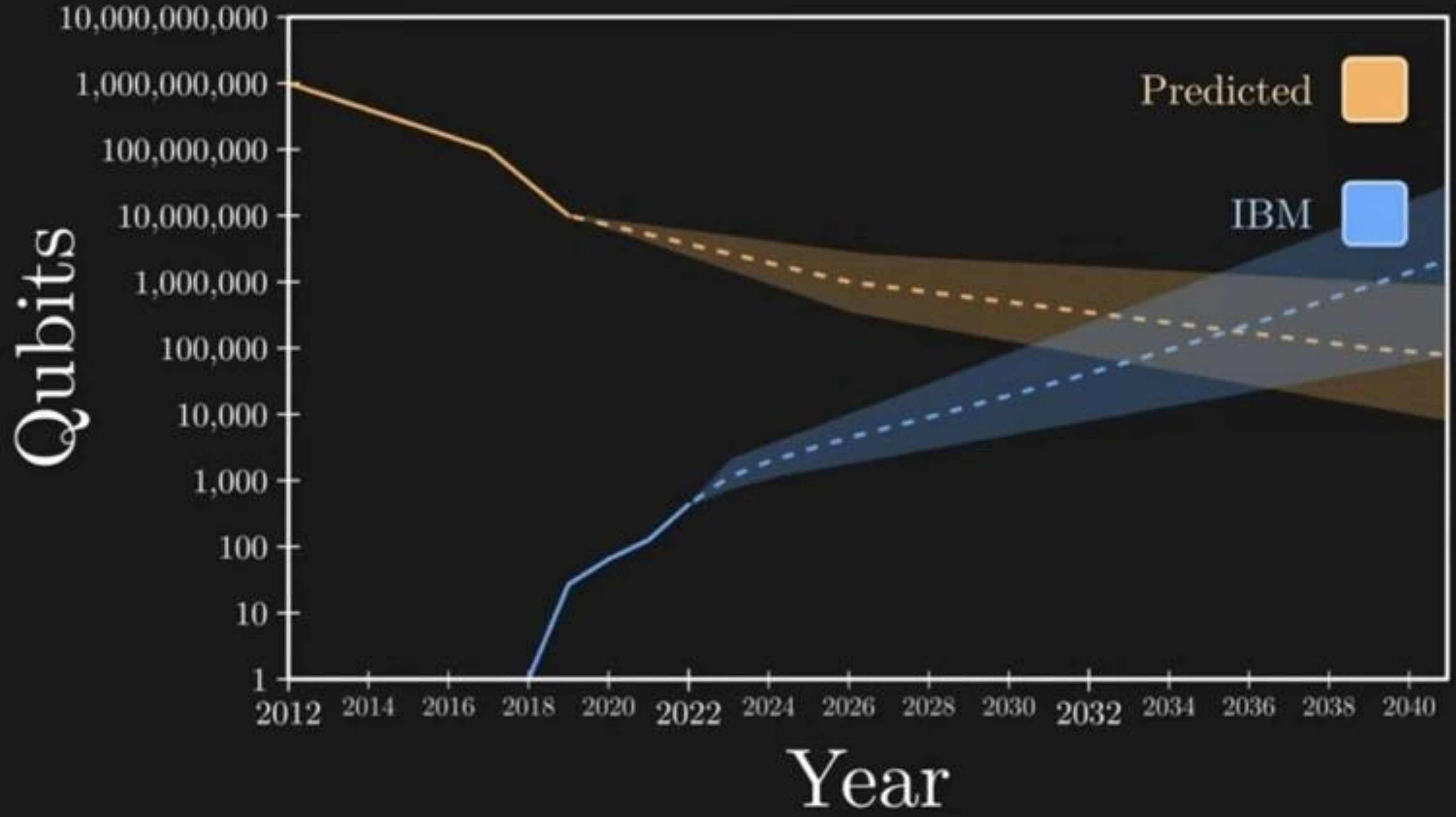
Photonics

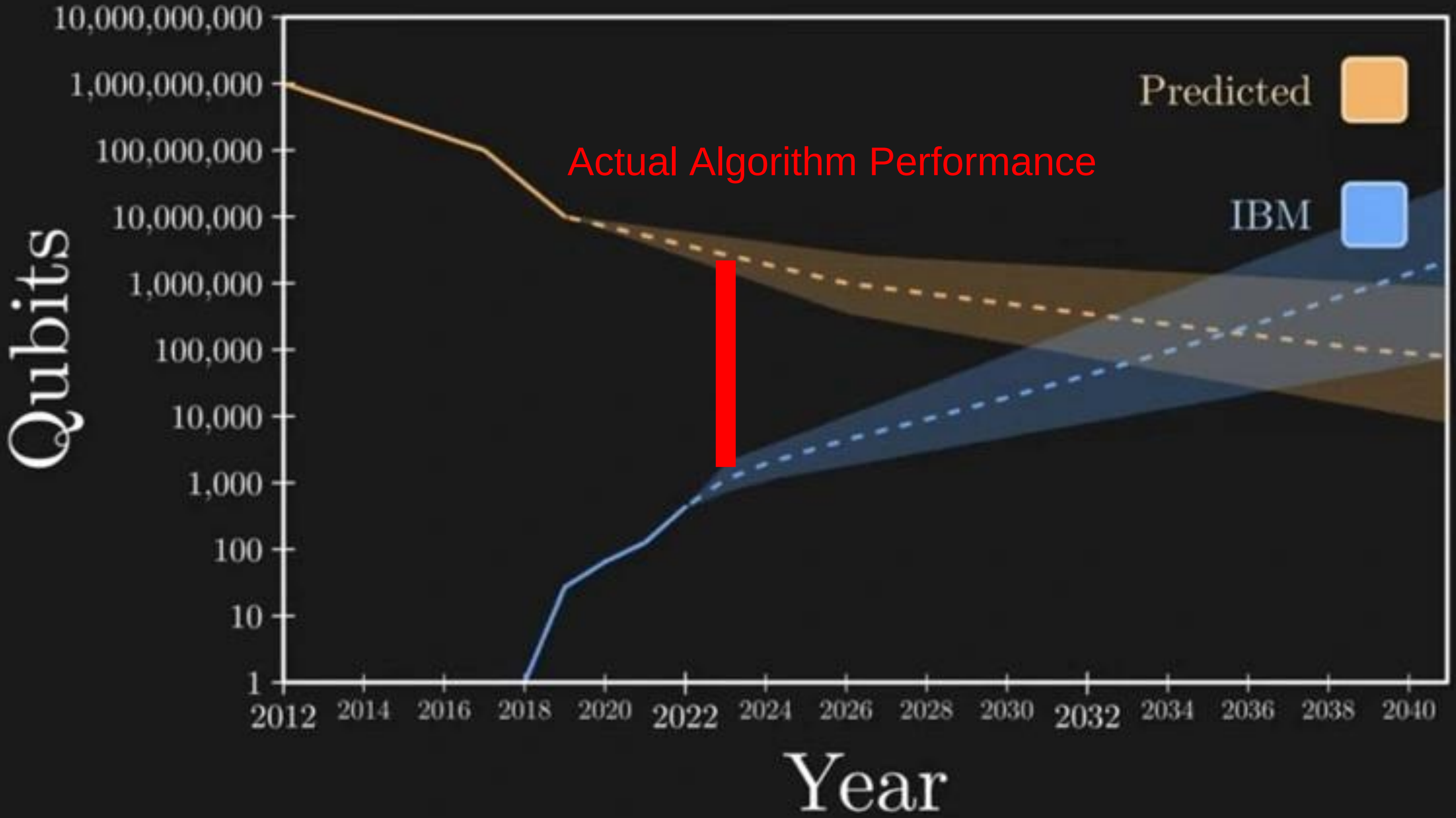
- PsiQuantum
- Rotonium
- Quantum Source
- QCi
- XANADU
- ORCA COMPUTING
- QUANDELA
- LightOn
- TuringQ
- QC82

Source: The Quantum Insider Intelligence Platform

Riverlane’s Quantum Error Correction Roadmap

	2023 Deltaflow 1 ✓	2024 Deltaflow 2	2025 Deltaflow 3	2026 Deltaflow Mega
QuOps	1,000	10,000	100,000	1,000,000
Functionality	**Fast decoding** Solving the backlog problem	**Streaming high-fidelity memory** Keeping the qubits alive forever	**Streaming logic** Enabling perpetual operations	**Logic at scale** First fully error-corrected quantum applications
Product Features	**Stability & memory** - First MHz decoder - Automated data flow - Bespoke interfacing	**Quantum memory** - Streaming real-time decoding - Leakage aware decoding - First universal interfacing	**Quantum gates** - Fast logic by lattice surgery - Fast logic by transversal gates - Higher error suppression rates - First logical orchestration	**Universal gate set** - Universal surface-code computation - Dynamic large-scale orchestration - Low-overhead real-time decoding supporting qLDPC codes


Qubits
10,000,000,000
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
2012
2014
2016
2018
2020
2022
2024
2026
2028
2030
2032
2034
2036
2038
2040
Year
Predicted
IBM



Actual Algorithm Performance

ELI5 of new Quantum Algorithms

Instead of breaking Bitcoin with a very large Quantum Computer we can’t build for 8-10 years, we can now use mass produced hardware currently in manufacturing process.

Active Volume

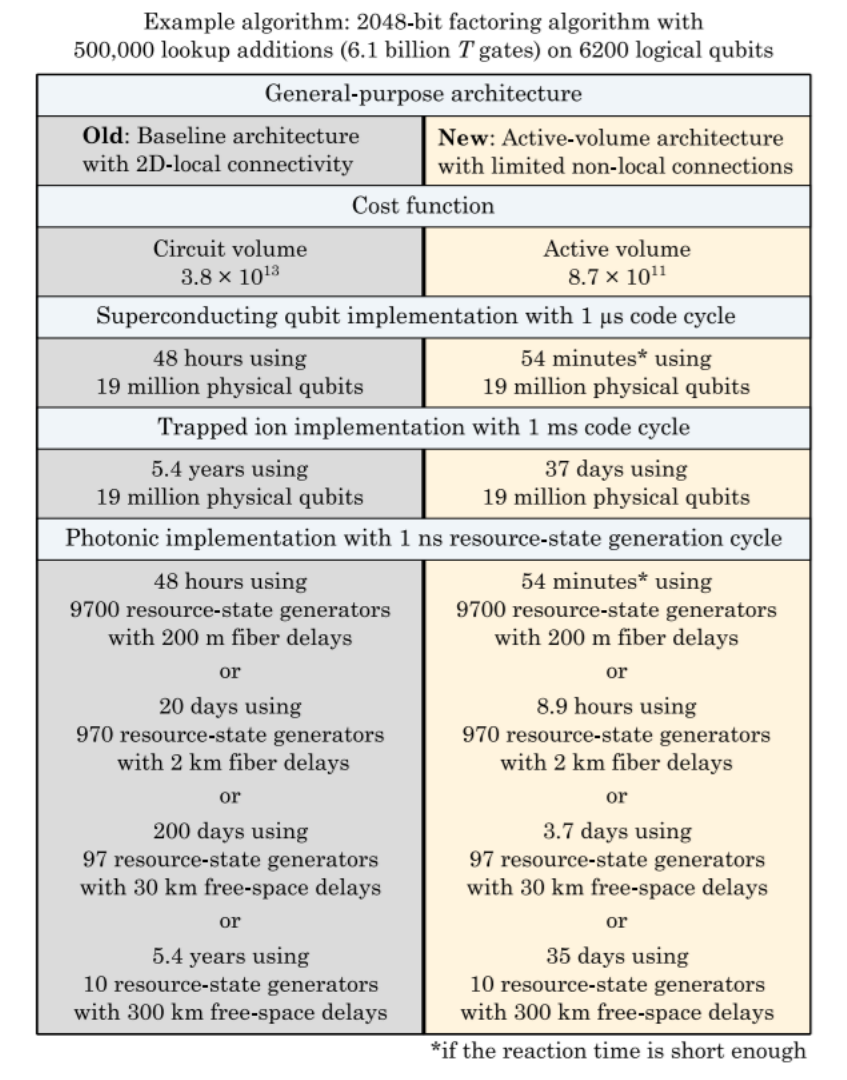
Litinski 2022 https://arxiv.org/pdf/2211.15465

Network based on implementation of algorithm and not all qubits connected

Faster than the same qubit count physically

Connected into a single machine.

Many small machines, not one big one



Example algorithm: 2048-bit factoring algorithm with 500,000 lookup additions (6.1 billion T gates) on 6200 logical qubits

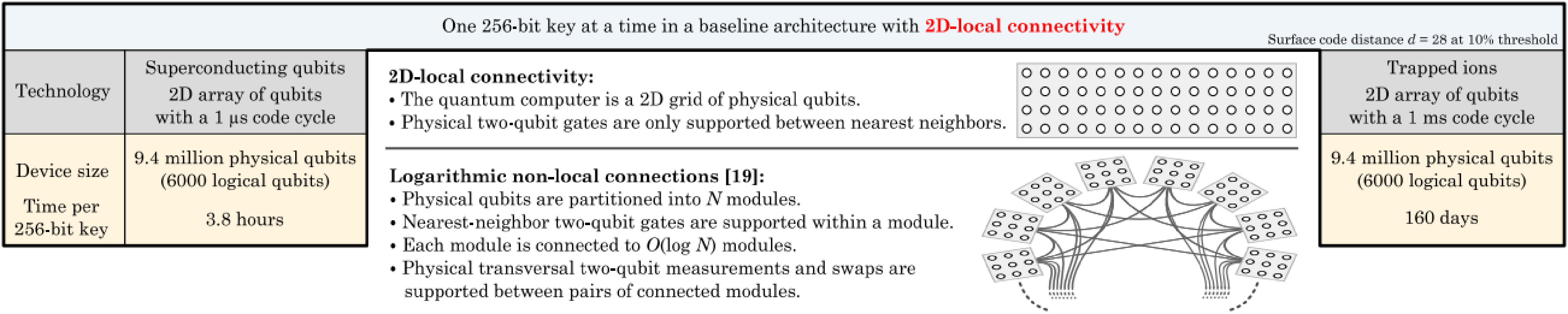
General-purpose architecture	
Old: Baseline architecture with 2D-local connectivity	**New**: Active-volume architecture with limited non-local connections
Cost function	
Circuit volume 3.8×10^{13}	Active volume 8.7×10^{11}
Superconducting qubit implementation with 1 μs code cycle	
48 hours using 19 million physical qubits	54 minutes* using 19 million physical qubits
Trapped ion implementation with 1 ms code cycle	
5.4 years using 19 million physical qubits	37 days using 19 million physical qubits
Photonic implementation with 1 ns resource-state generation cycle	
48 hours using 9700 resource-state generators with 200 m fiber delays or 20 days using 970 resource-state generators with 2 km fiber delays or 200 days using 97 resource-state generators with 30 km free-space delays or 5.4 years using 10 resource-state generators with 300 km free-space delays	54 minutes* using 9700 resource-state generators with 200 m fiber delays or 8.9 hours using 970 resource-state generators with 2 km fiber delays or 3.7 days using 97 resource-state generators with 30 km free-space delays or 35 days using 10 resource-state generators with 300 km free-space delays

*if the reaction time is short enough

https://arxiv.org/pdf/2306.08585 Litinski 2023 “How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates”

Targeting BTC block time on average, solving Bitcoin’s UTXO public key into private key with enough time to front run the transaction and send the money to the attacker.

2D local is “one giant machine” and the time predicted is 3.8 hours with 6000 logical qubits on superconducting (IBM, Google, Alice and Bob) qubits, or 160 days with Trapped Ion (Quantinuum, Oxford Ionics)



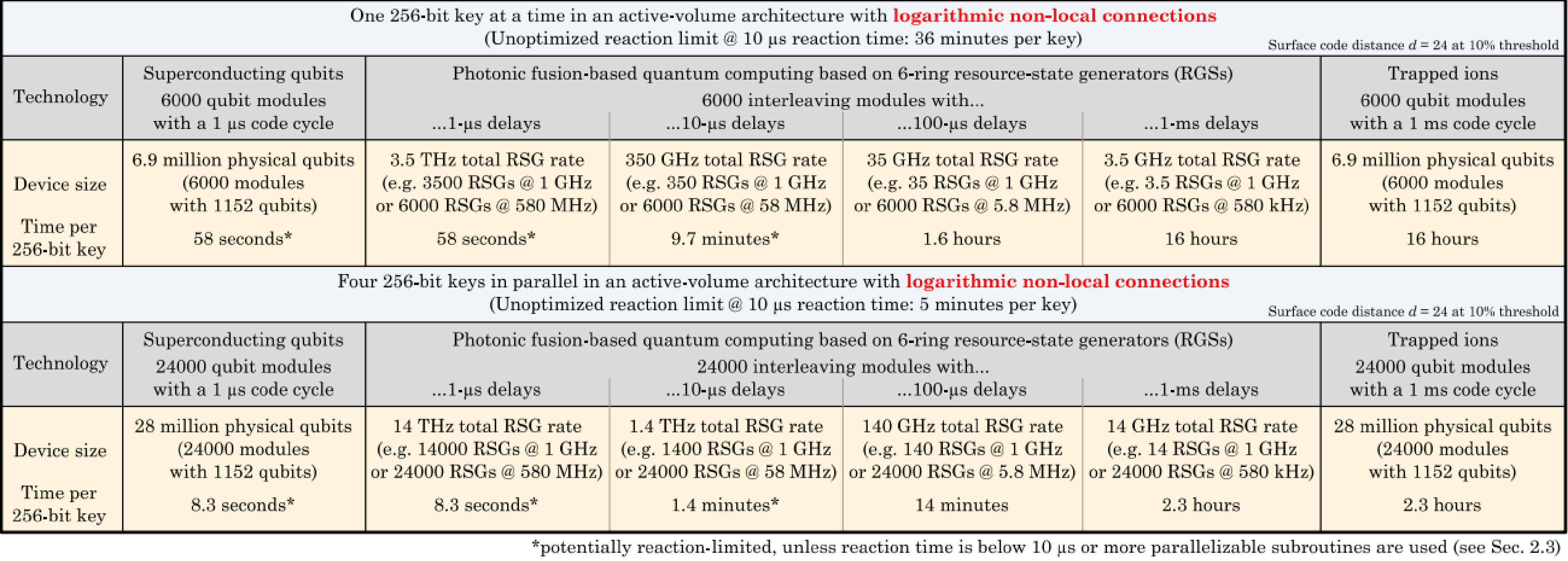
One 256-bit key at a time in a baseline architecture with **2D-local connectivity**

Surface code distance $d = 28$ at 10% threshold

Technology	Superconducting qubits 2D array of qubits with a 1 μs code cycle	Trapped ions 2D array of qubits with a 1 ms code cycle
Device size	9.4 million physical qubits (6000 logical qubits)	9.4 million physical qubits (6000 logical qubits)
Time per 256-bit key	3.8 hours	160 days

2D-local connectivity:
- The quantum computer is a 2D grid of physical qubits.
- Physical two-qubit gates are only supported between nearest neighbors.

Logarithmic non-local connections [19]:
- Physical qubits are partitioned into N modules.
- Nearest-neighbor two-qubit gates are supported within a module.
- Each module is connected to $O(\log N)$ modules.
- Physical transversal two-qubit measurements and swaps are supported between pairs of connected modules.



One 256-bit key at a time in an active-volume architecture with **logarithmic non-local connections**
(Unoptimized reaction limit @ 10 μs reaction time: 36 minutes per key)

Surface code distance $d = 24$ at 10% threshold

Technology	Superconducting qubits 6000 qubit modules with a 1 μs code cycle	Photonic fusion-based quantum computing based on 6-ring resource-state generators (RGSs) 6000 interleaving modules with...				Trapped ions 6000 qubit modules with a 1 ms code cycle
		...1-μs delays	...10-μs delays	...100-μs delays	...1-ms delays	
Device size	6.9 million physical qubits (6000 modules with 1152 qubits)	3.5 THz total RSG rate (e.g. 3500 RSGs @ 1 GHz or 6000 RSGs @ 580 MHz)	350 GHz total RSG rate (e.g. 350 RSGs @ 1 GHz or 6000 RSGs @ 58 MHz)	35 GHz total RSG rate (e.g. 35 RSGs @ 1 GHz or 6000 RSGs @ 5.8 MHz)	3.5 GHz total RSG rate (e.g. 3.5 RSGs @ 1 GHz or 6000 RSGs @ 580 kHz)	6.9 million physical qubits (6000 modules with 1152 qubits)
Time per 256-bit key	58 seconds*	58 seconds*	9.7 minutes*	1.6 hours	16 hours	16 hours

Four 256-bit keys in parallel in an active-volume architecture with **logarithmic non-local connections**
(Unoptimized reaction limit @ 10 μs reaction time: 5 minutes per key)

Surface code distance $d = 24$ at 10% threshold

Technology	Superconducting qubits 24000 qubit modules with a 1 μs code cycle	Photonic fusion-based quantum computing based on 6-ring resource-state generators (RGSs) 24000 interleaving modules with...				Trapped ions 24000 qubit modules with a 1 ms code cycle
		...1-μs delays	...10-μs delays	...100-μs delays	...1-ms delays	
Device size	28 million physical qubits (24000 modules with 1152 qubits)	14 THz total RSG rate (e.g. 14000 RSGs @ 1 GHz or 24000 RSGs @ 580 MHz)	1.4 THz total RSG rate (e.g. 1400 RSGs @ 1 GHz or 24000 RSGs @ 58 MHz)	140 GHz total RSG rate (e.g. 140 RSGs @ 1 GHz or 24000 RSGs @ 5.8 MHz)	14 GHz total RSG rate (e.g. 14 RSGs @ 1 GHz or 24000 RSGs @ 580 kHz)	28 million physical qubits (24000 modules with 1152 qubits)
Time per 256-bit key	8.3 seconds*	8.3 seconds*	1.4 minutes*	14 minutes	2.3 hours	2.3 hours

*potentially reaction-limited, unless reaction time is below 10 μs or more parallelizable subroutines are used (see Sec. 2.3)

A lot of little machines is much faster: 6000 modules with **1152 qubits** each is 58 seconds for superconducting, 16 hours for trapped ions. Based on the networking delays and gate speed, photonics are 58 seconds to 17 hours (limited by speed of light in fiber) 24000 modules with **1152 qubits** each is 8.3 seconds solve time.

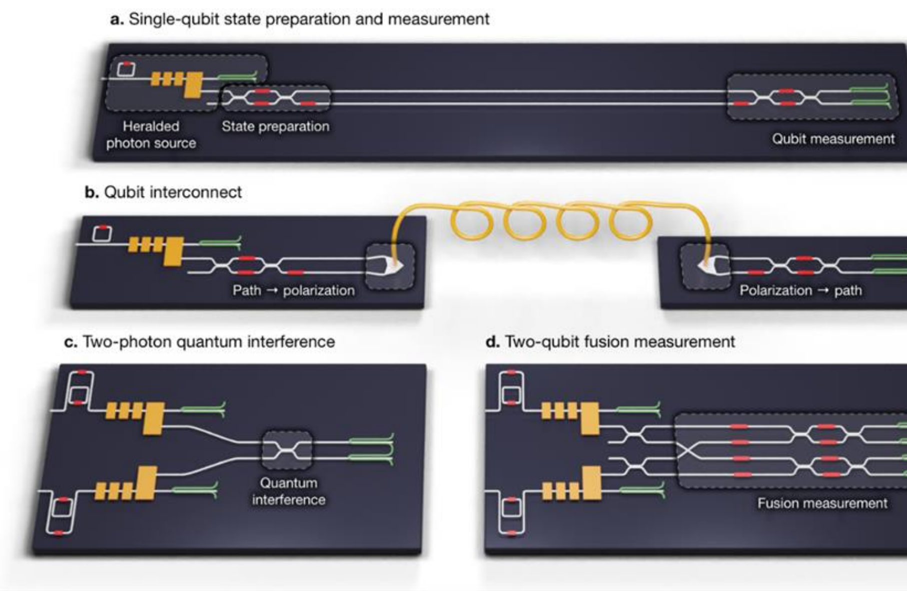
Quantum Computers enter Mass Production

PSIQuantum 26 April 2024: A manufacturable platform for photonic quantum computing https://arxiv.org/html/2404.17570v1

GlobalFoundries 5 May 2024: PsiQuantum and GlobalFoundries to Build the World's First Full-scale Quantum Computer

https://gf.com/dresden-press-release/psiquantum-and-globalfoundries-build-worlds-first-full-scale-quantum-computer/

OXFORD, 11 July 2024: Scalable, high-fidelity all-electronic control of trapped-ion qubits https://arxiv.org/abs/2407.07694



Traditional Semiconductor manufacturing facilities are used to build BTC/ ETH / SOL breaking quantum computers

Timeline ?

No more science left for PSIQuantum, just manufacturing

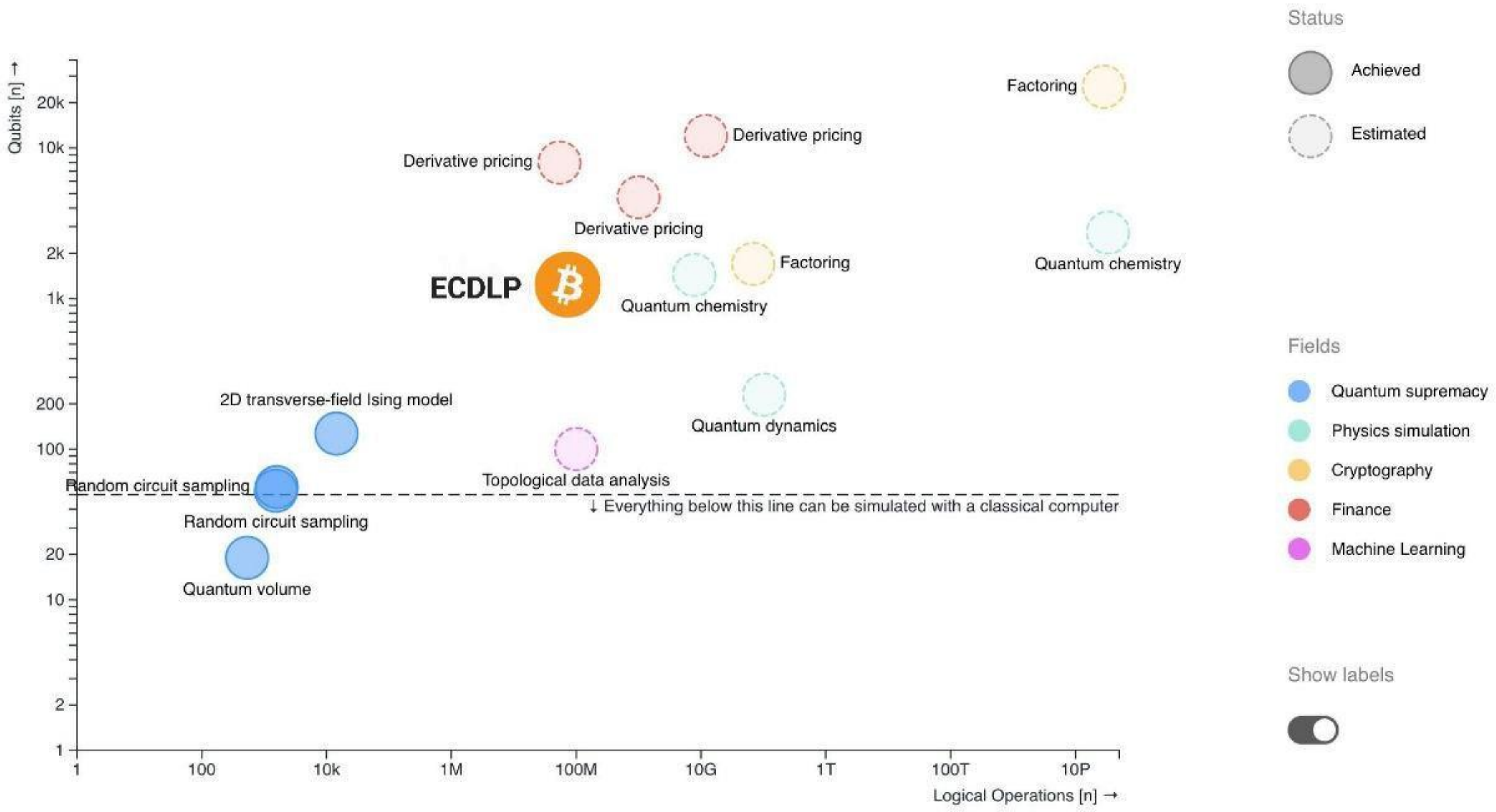
1 facility in upstate New York can make 500,000 devices per year. QDay 2027

Hiring for testing personnel at 4 more facilities. 3 facilities moves to QDay 2026

5-10 Companies are targeting 2027 for 1 million qubits

More improvement possible in algorithms explained by Litinski in his Youtube presentation at QIP2024 www.youtube.com/watch?v=AumHpDRS5iI

Quantum Computers: What We Need and What We Have



What does “broken” mean for QDay?

Public keys converted into the Private key by Discrete Log problem, using Shor’s Algorithm

If a transaction has been performed from an address, the public key is exposed.

Money can be spent from wallet, no matter cold storage or hot storage.

UTXO protects against ECDLP by creating new addresses. Ethereum / Solana can do the same but interacting with smart contracts will expose public key.

Attackers can still steal funds from UTXO if the solve time is fast enough.

Multi-sig are the most exposed, so BLS and Shamir Secret Sharing are gone

What does QDay mean for Web3?

QDay is “provable” to everyone when Satoshi’s old coins move.
20-30% of BTC coins have exposed public keys. (p2pk addresses and not p2pkh, plus address reuse.)

4-6 million BTC ($240 billion) would be up for sale, and the price will drop

About $1.7 Trillion in Layer 1 / Layer 2 chains. About $70 Billion in DeFi.

USDC has a circulating supply of **$35B**

USDT has a circulating supply of **$115B**

150 / 1700 = 8% of TVL

92% not enough fiat, assuming all Circle and Tether can withdraw.

The value of Web3 assets will quickly trend towards zero, or 1 BTC = 1 pizza

Opportunity

Partially migrated systems (like BTC p2pk to p2pkh) will still leave huge amounts of value to attack. **Burning all old wallets** would be required, but that also burns the users, contracts, bridges, etc and does not make the ecosystem safe still.

Make a new, fresh, clean **Quantum Safe** ecosystem. QuantumEVM.com

New qWeb3 means new #1 DEX, #1 DeFi, #1 Markets

Even if $200 million was spent today in advertising a new DEX, Uniswap would still be the King.

Migrate contracts early as a backup. When the users migrate to safety, new King.

Requirements

Must discard all ECC based Cryptography. No more zkSNARKS or FHE w/ECC

Use cryptography that is safe from Quantum Computers - no more weaknesses.

Lattices, Codes, Hashes (SHA256, SHA3, Blake2b, etc) are safe

NIST Post Quantum Competition ran since 2015 and many systems were attacked for years. There is variety and opportunity.

Signal, Apple, Google Chrome already migrated to Post Quantum Cryptography.

SSL (and banks) have a very easy migration from the SSL key distribution

Cars, missiles, IoT have a harder problem with distributed hardware and networks.

Networks

Cellframe.net is a layer 0 with NIST PQ with Sharding and Network-of-Networks.
Python Plugins

QuantumEVM.com is a Layer 1 built on Cellframe. EVM smart contracts

KelVPN.com is a Layer 1 built on Cellframe, PQ VPN run by staking nodes

TheQRL.org is a hash based Layer 1, no smart contracts

Abelian.info is PQ crypto Layer 1, no smart contracts

Some networks are mid-migration (CKB L2 at 0%, Algorand L1 at 0%)

Other networks are not recommended for various reasons