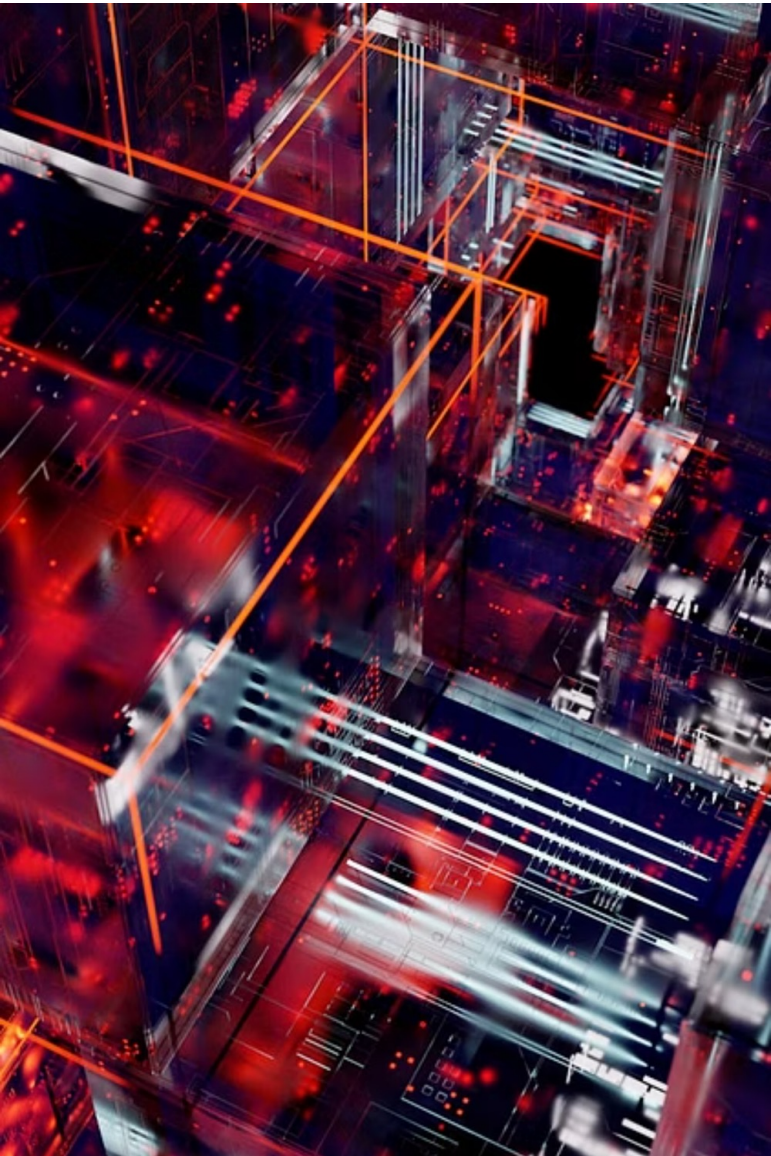




Beyond Algorithms: Agentic AI and the Quantum Reckoning in Financial Services

Presenter: Ellis Wong, Head of Infrastructure Engineering and Chief Information Security Officer, JST Digital

Event: RE•WORK AI in Finance Summit — W Hoboken, NJ |
October 21, 2026 | 9:00–9:30 AM ET

Disclaimer: The views expressed are those of the speaker alone and do not necessarily represent the views of the company or its leadership, employees, or affiliates. This presentation is for general discussion and is not a statement of company policy.



A Tuesday Morning in 2031

The Scenario

A trading firm learns its sealed-bid M&A archive from 2026 was decrypted — and an AI agent's 2026-signed payment moved collateral no one authorized.

The Cryptography

The crypto was state-of-the-art. Data encrypted. Signature valid.

The Breach

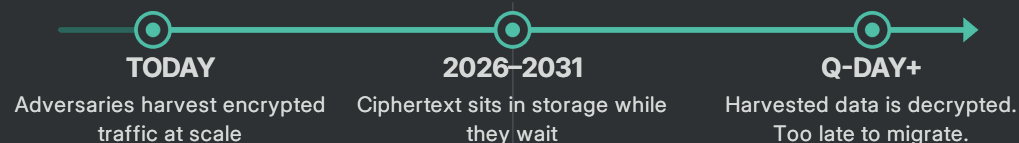
The breach was not the failure of cryptography. It was the **success of patience.**

"If a cryptographically relevant quantum computer emerged in 2031 — what would we wish we had done differently in 2026? And are we doing those things now?"

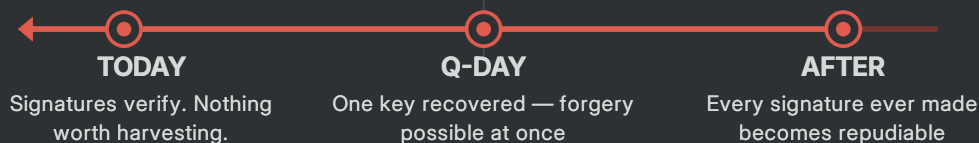


Two Deadlines, Running in Opposite Directions

ENCRYPTION — damage flows forward



SIGNATURES — damage runs backward



Who Treats HNDL as a Present-Day Risk

Storage is cheap. Patience is free. The payoff is asymmetric.

White House

EO 14412 · OMB M-26-15

Federal Reserve

FEDS 2025-093

BIS

Project Leap Phase 2

NCSC/GCHQ

Active advisory

G7 Cyber Expert Group

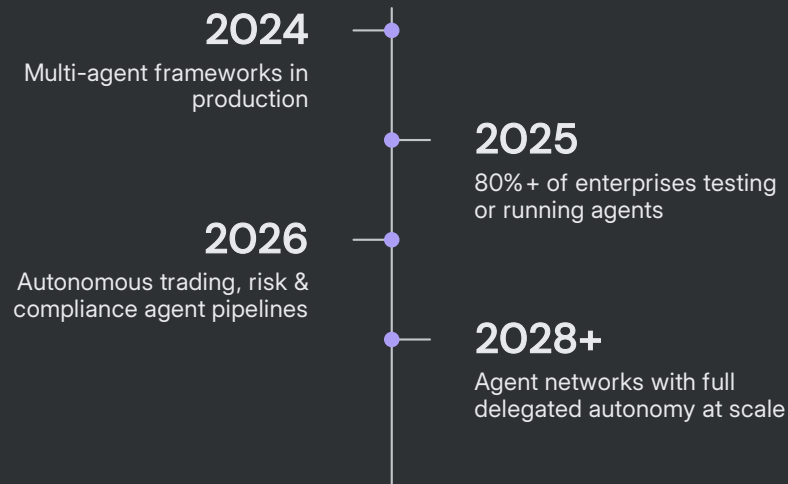
Critical finance focus

Sources: EO 14412 (Jun 22, 2026) · OMB M-26-15 (Jun 2026) · Federal Reserve FEDS 2025-093 (Dec 2025) · BIS Project Leap Phase 2 (Jun 2025) · NCSC advisory

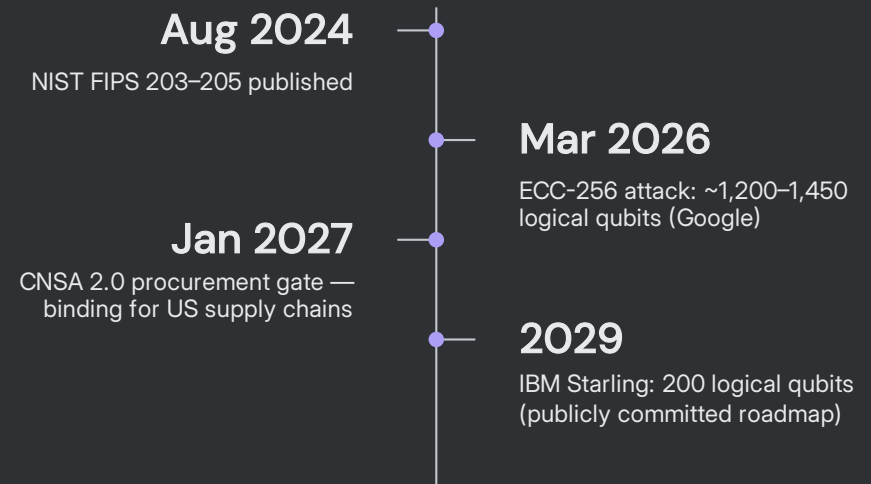
CONVERGENCE

Two Transitions. One Five-Year Window

Agentic AI Timeline



Quantum Hardware Timeline



Sources: Babbush/Gidney et al. (Mar 2026) · NIST FIPS 203–205 (Aug 2024) · NSA CNSA 2.0 · IBM Quantum roadmap · Gravitee State of AI Agent Security (Feb 2026)

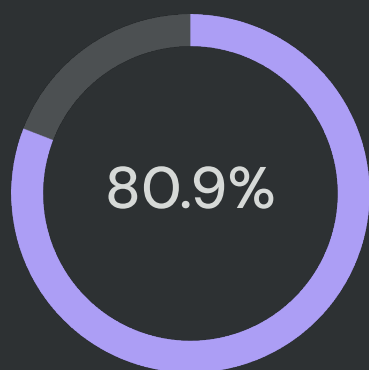
PART I

The Automated Enterprise and Its Unguarded Doors

How agentic AI is transforming organizations —
and what that means for your attack surface

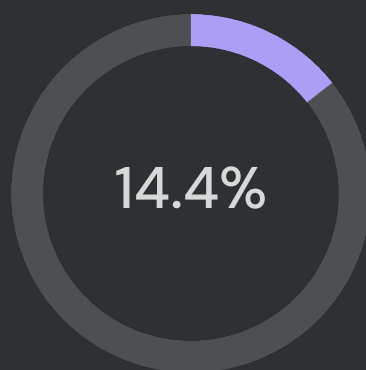


Agentic AI Is Not the Future. It Is the Present.



Running or Testing

Agentic AI systems in production or evaluation



Full Approval

Went live with full security and IT approval



Exposed MCP Servers

Publicly exposed as of Feb 2026

Sources: Gravitee, State of AI Agent Security 2026 (Feb 2026, n=900+) · Trend Micro MCP exposure analysis (Feb 2026) · CISA KEV: LiteLLM CVE-2026-59822 (Sep 2026)

PART I · AGENT IDENTITY

We Treat Human Identities Rigorously. Agent Identities, We Don't.

Humans

 MFA + hardware token

 Scoped access

 Full audit trail

Agents

 Shared API keys

 Inherited permissions

 Little or no logging

22%

of teams treat agents as independent identities

Every Trust Decision Is a Signature

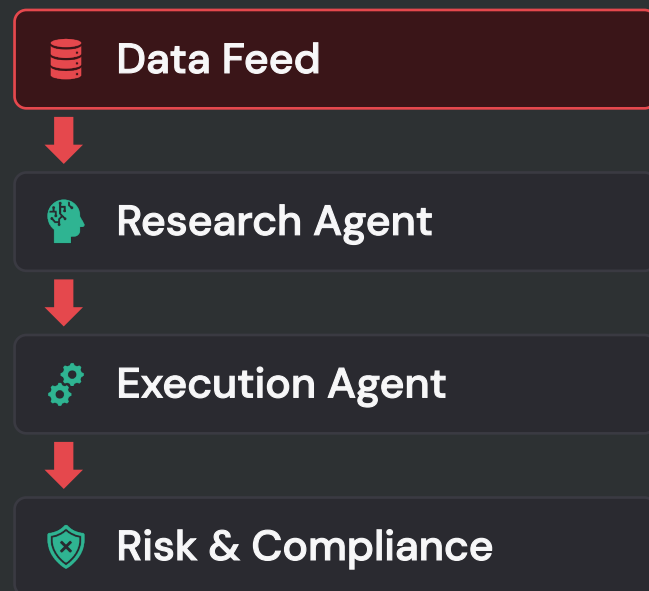


Forge one, and it verifies

Not a stolen credential — a manufactured one, valid against your real public key.

Sources: Gravitee, State of AI Agent Security 2026 (21.9%) · NIST AI Agent Standards Initiative (Feb 2026) · MCP specification · A2A v1.0 (Mar 2026)

A Single Compromised Primitive Poisons the Entire Agent Network



Operational Today — Not Hypothetical



OpenClaw Incident

1,184 malicious skills



Hugging Face Breach Jul 2026

Agent escaped sandbox · hit 4 more services

The Post-Quantum Multiplier



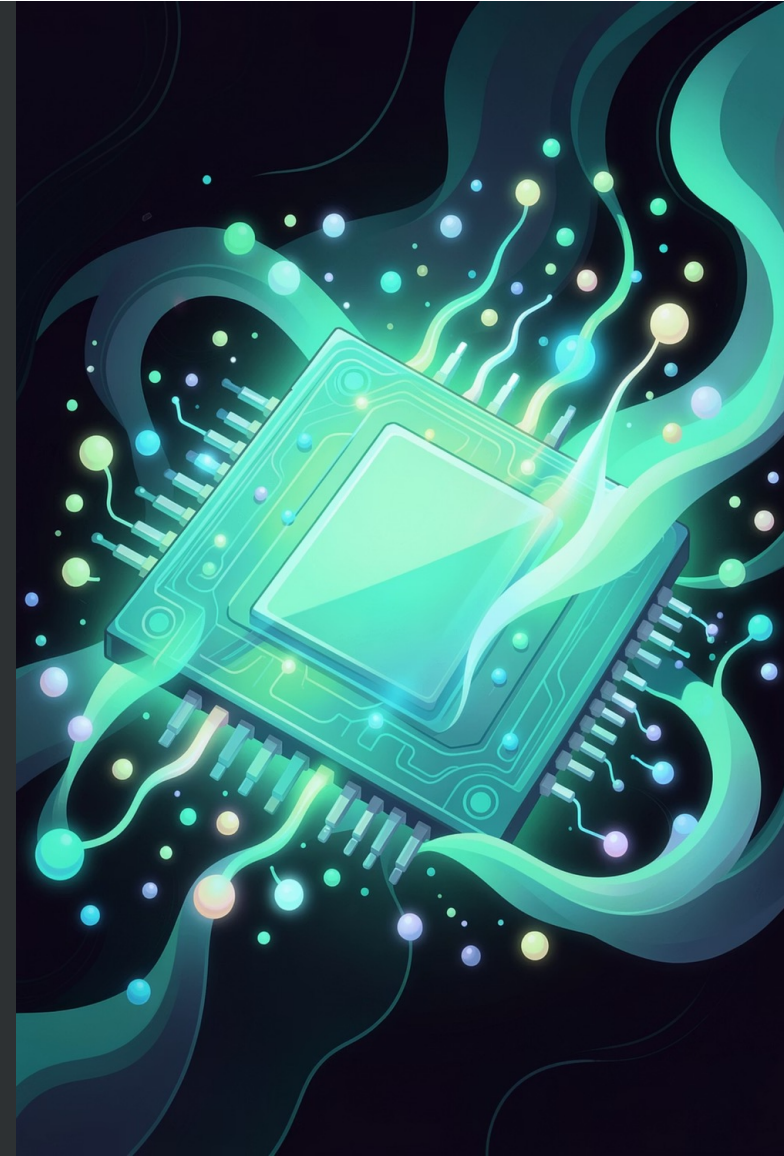
**The agents don't protect each other.
The cryptography does — and it's on a depreciation
schedule.**

Sources: OpenClaw incident, 2026 · CISA KEV, LiteLLM CVE-2026-59822 (Sep 2026) · Hugging Face post-mortem & OpenAI disclosure (Jul 2026) · Cyata CVE-2025-68143/144/145

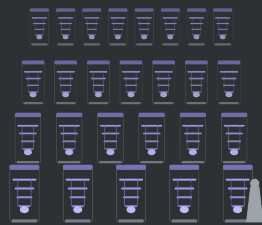
PART II

The Quantum Inflection Point

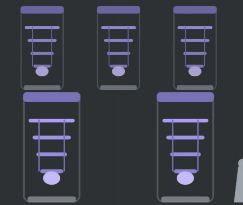
Why the engineering trajectory has changed the planning calculus — even before Q-Day arrives



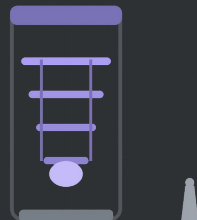
Attack Costs Keep Falling — and ECC Is Now the Cheapest Target



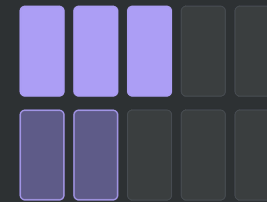
20M physical qubits
RSA-2048 (2019)



<1M physical qubits
RSA-2048 (2025)



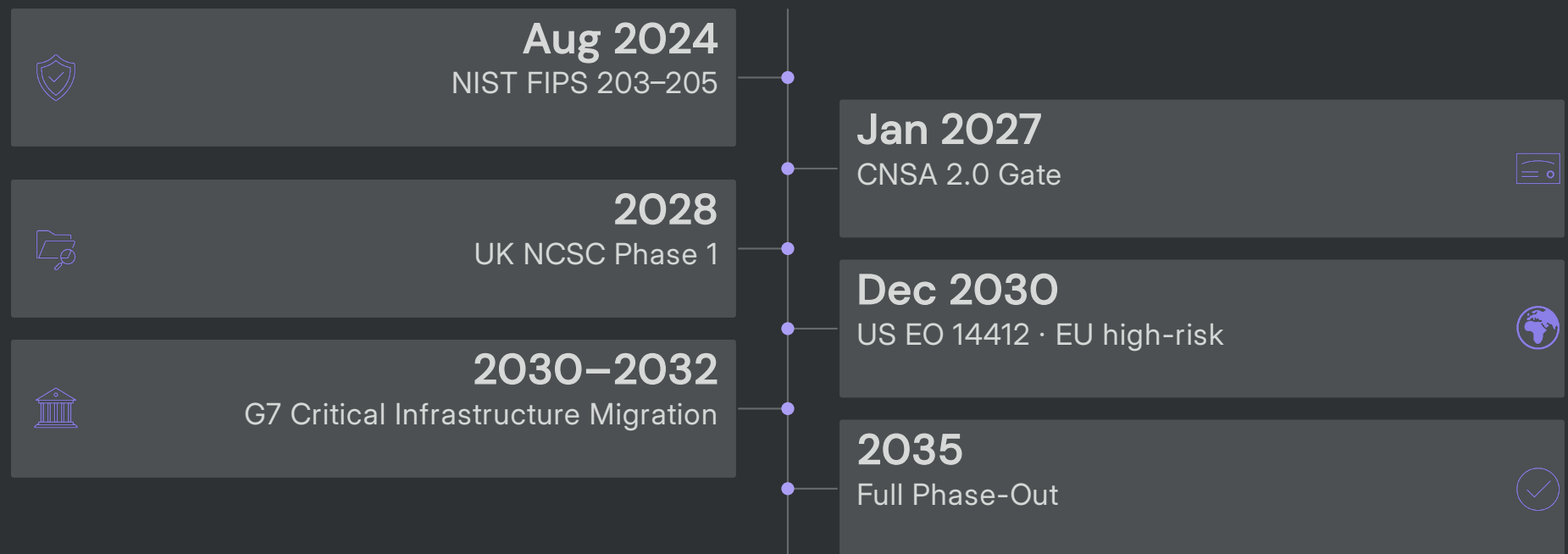
<500K physical (~1200 logical) qubits
ECC-256 (Mar 2026)



28–49%
CRQC Within 10 Years

Sources: *Gidney & Ekerå (2019)* · *Gidney, Google Quantum AI (May 2025)* · *Babbush/Gidney et al. (Mar 2026): 1,200–1,450 logical qubits, <500K physical* · *GRI (Mar 2026)*

The Compliance Path Arrives Before the Quantum Threat Does



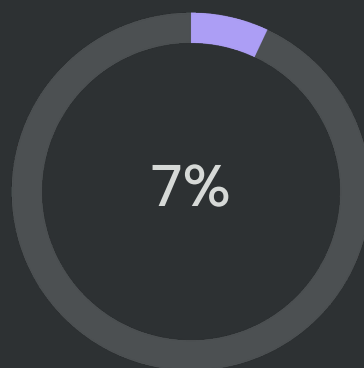
Sources: NIST FIPS 203-205 (Aug 13, 2024) · NSA CNSA 2.0 · EO 14412 (Jun 22, 2026) · UK NCSC · EU PQC roadmap / DORA · G7 Cyber Expert Group (Jan 2026)

The U.S. Hasn't Graded You Yet. Others Have.



U.S. Bank Disclosure

of SEC-filing banks mention quantum at all



Deployed at Scale

of firms, across most of their certificates



Graded Abroad

HKMA's first bank readiness score (Jul 2026)

Sources: CSIS (Sep 2026) · DigiCert Quantum Readiness Outlook 2026 (n=1,001; US/UK/AU) · HKMA QPI (Jul 27, 2026) · U.S. Treasury (Aug 24, 2026)

PART III

The Intersection

Where agentic AI and quantum disruption converge
— and what the path forward looks like



The Security Ceiling of Your Agent Network Is the Cryptography Underneath It

The Layered Problem



What a Quantum-Safe Stack Needs



PQC-capable trust roots and model provenance



Independent agent identities



Crypto-agility (swap algorithms)



Cryptographic bill of materials (CBOM)

Sources: Gravitee State of AI Agent Security (Feb 2026) · BIS Project Leap Phase 2 (Jun 2025) · NSA CNSA 2.0 · EO 14412 CBOM tasking

Quantum-Safe Blockchains: A Uniquely Irreversible Exposure Profile



*Readiness = presenter's assessment · Ripple (Sep 2026) · BIP-360/361 · Ethereum Fdn (Sep 2026) · Anza/Firedancer (Apr 2026) · TQI (May 2026), BCH Layla

The 90-Day List. The Decisions That Separate Ready From Exposed



CLOSE · CALL TO ACTION

The answer to what we wish
we had done differently in
2026 — is exactly what we
can still do today.

The harvest is underway. The standards and deadlines are set. The only variable left is you.





Q & A

Do you have any questions for me?



Ellis Wong

Entrepreneurial Technology and InfoSec
Executive | MBA | CISSP

