PREPARING ETHEREUM FOR A POST-QUANTUM FUTURE

→ a coordination story

Will Corcoran | Research Coordinator, Ethereum Foundation

WHERE WE ARE GOING TODAY?

→ **PART 1** | Context Setting

→ **PART 2** | Quantum Computing 101

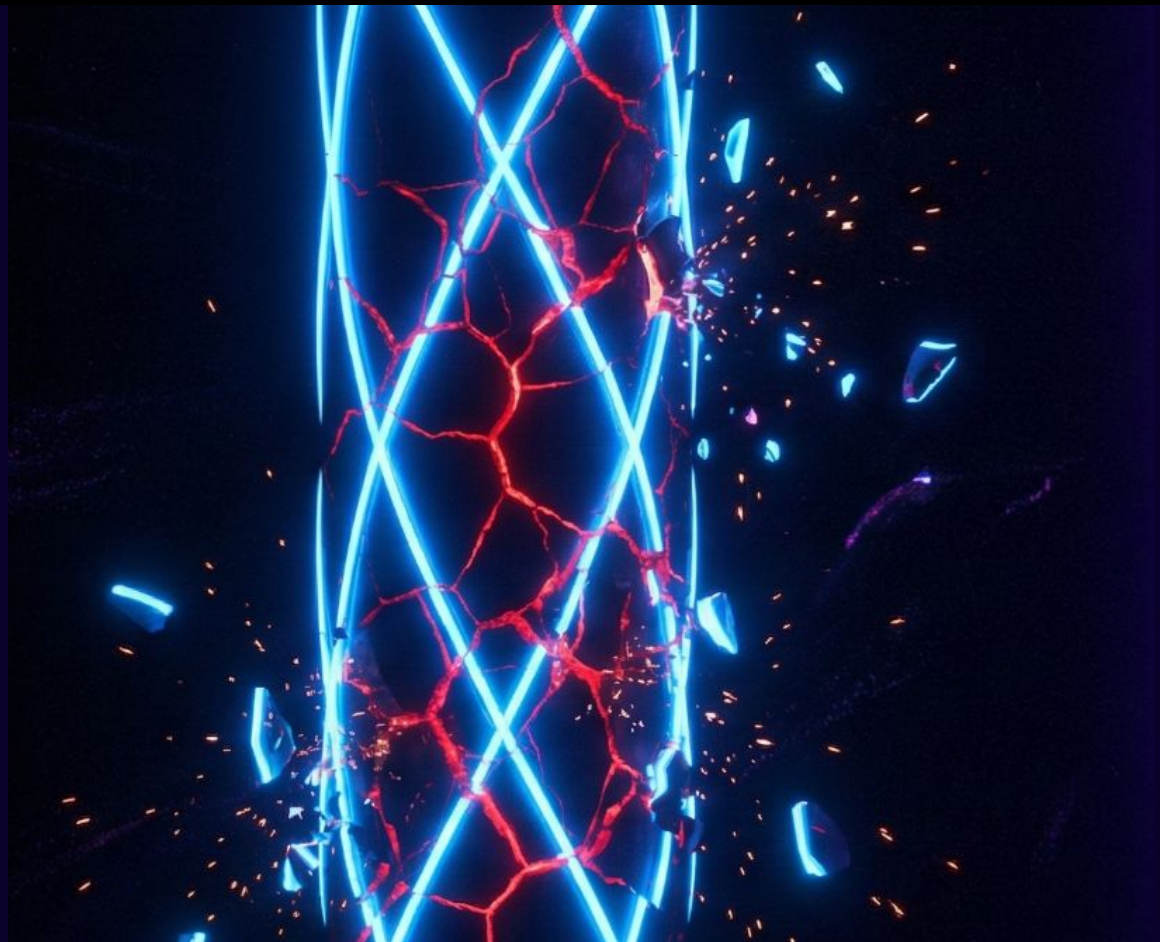
→ **PART 3** | The Size Problem

→ **PART 4** | The Solution

→ **PART 5** | The Effort

→ **PART 6** | Industry & L2 implications

BEFORE WE BEGIN—ECC IS TOAST



Part 1

CONTEXT SETTING

→ What EF research coordination looks like

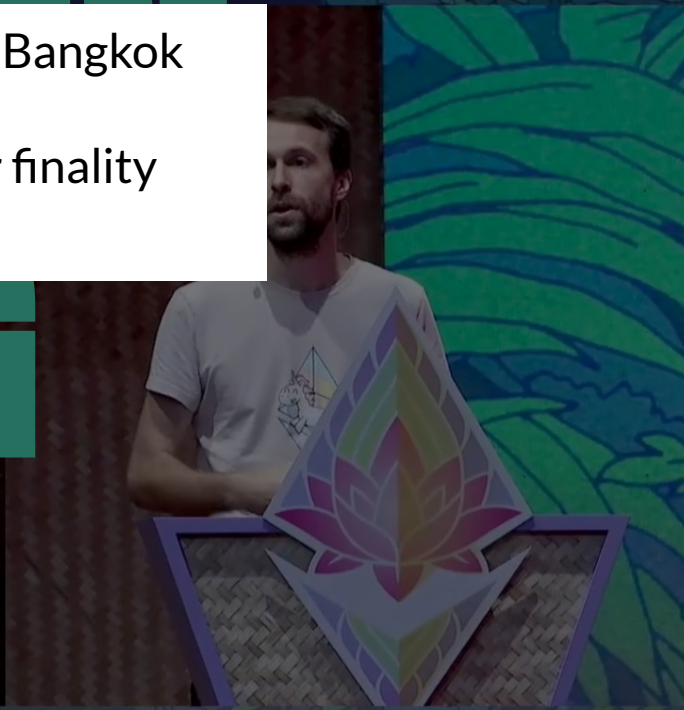
THE TALK THAT CHANGED EVERYTHING

2024

DC7 SEA

THE TALK THAT EVERYTHING

- → Nov 2024: Justin Drake's "beam chain" talk at Devcon Bangkok
- → A proposed redesign of Ethereum's consensus layer
- → Quantum security + real-time SNARKification + faster finality
- → My entry point



DC7 SEA

THE TALK THAT

2025

ERYTHING

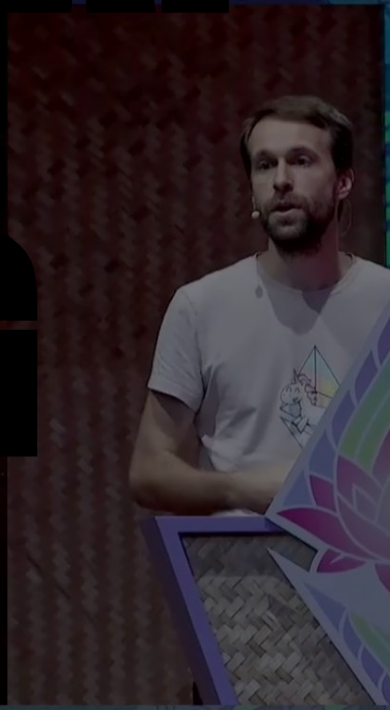
~~beam chain~~

lean Ethereum →

lean consensus

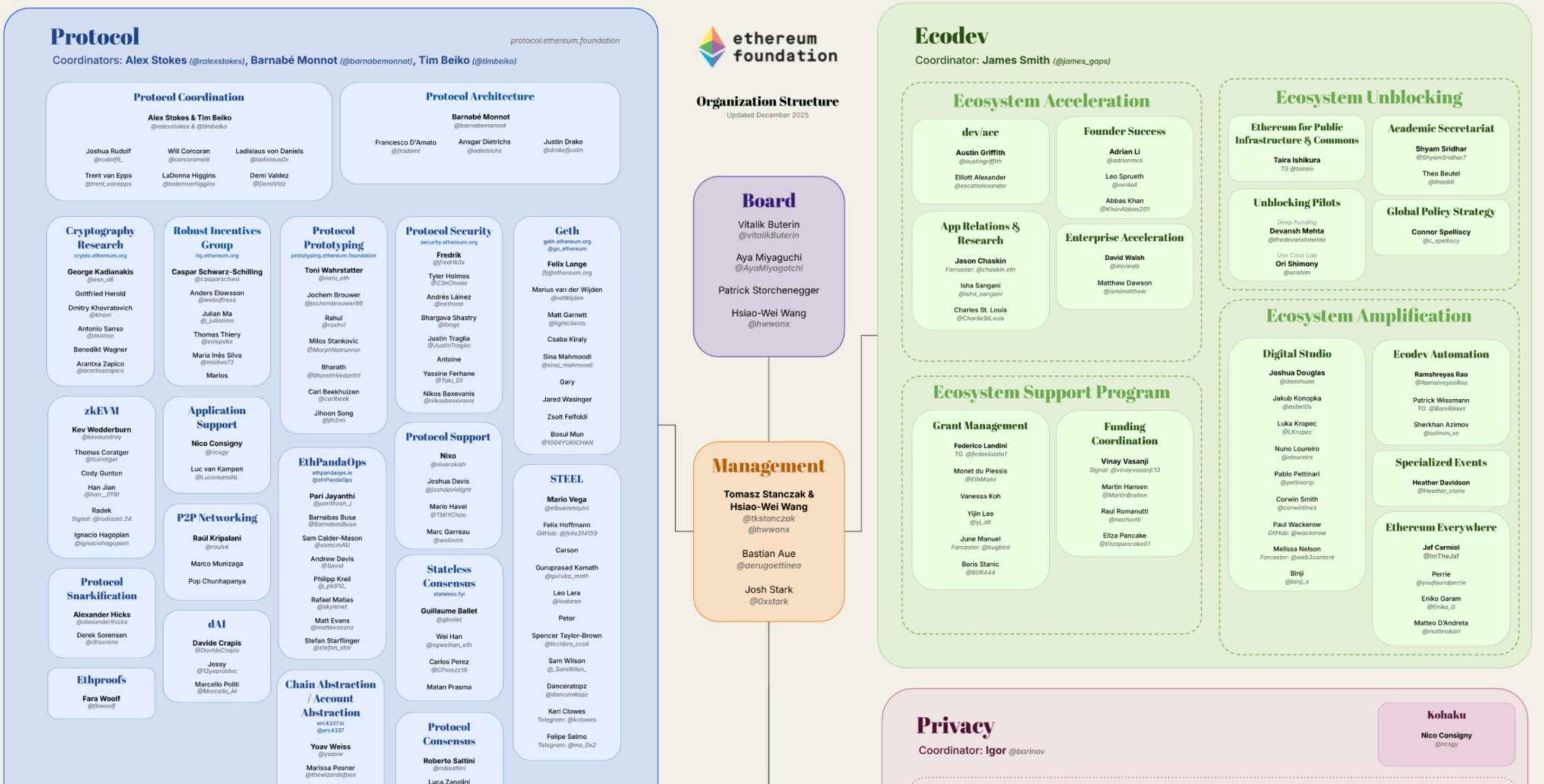
lean data

lean execution



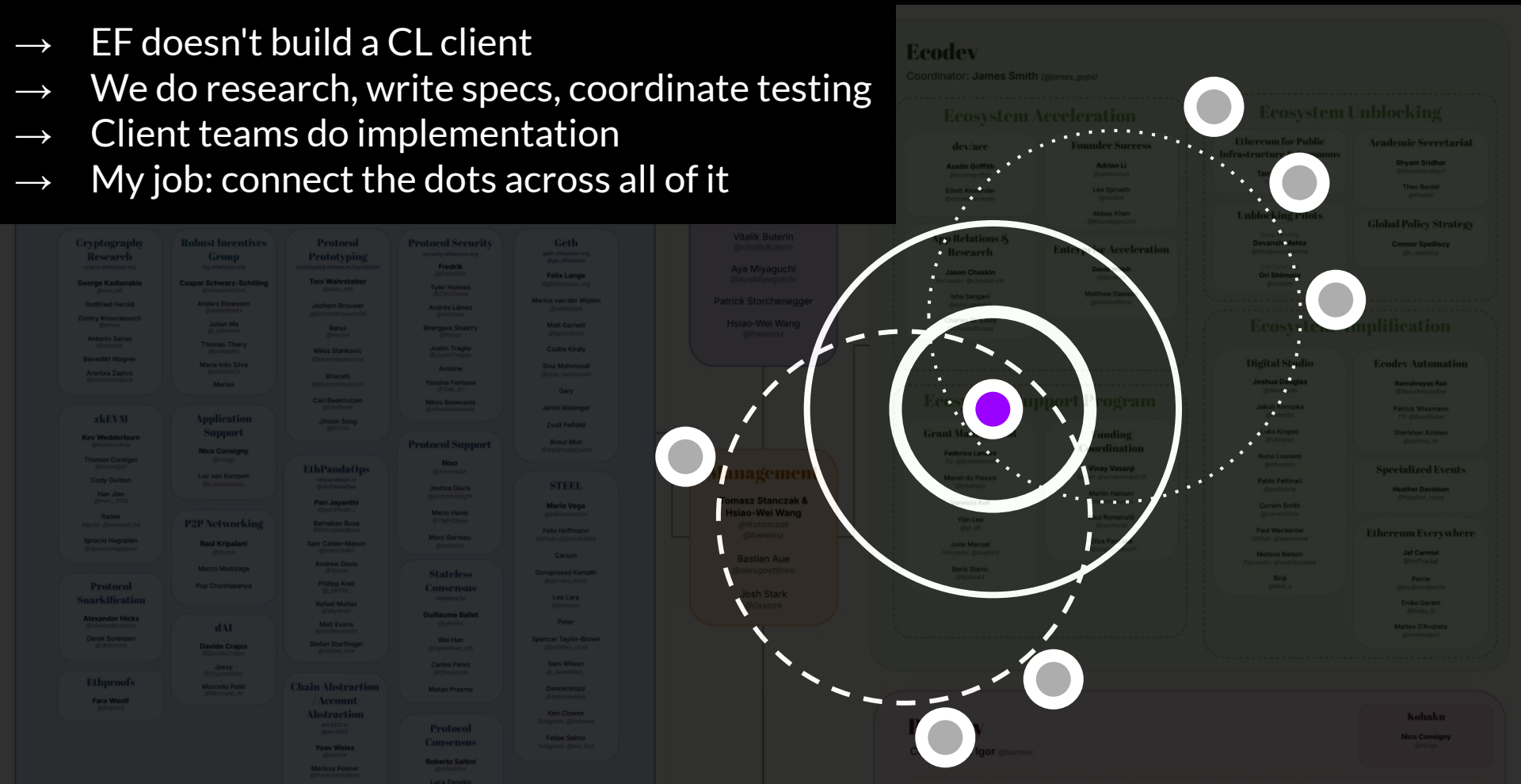
DC7 SEA

RESEARCH+SPECS+TESTING+COORDINATION



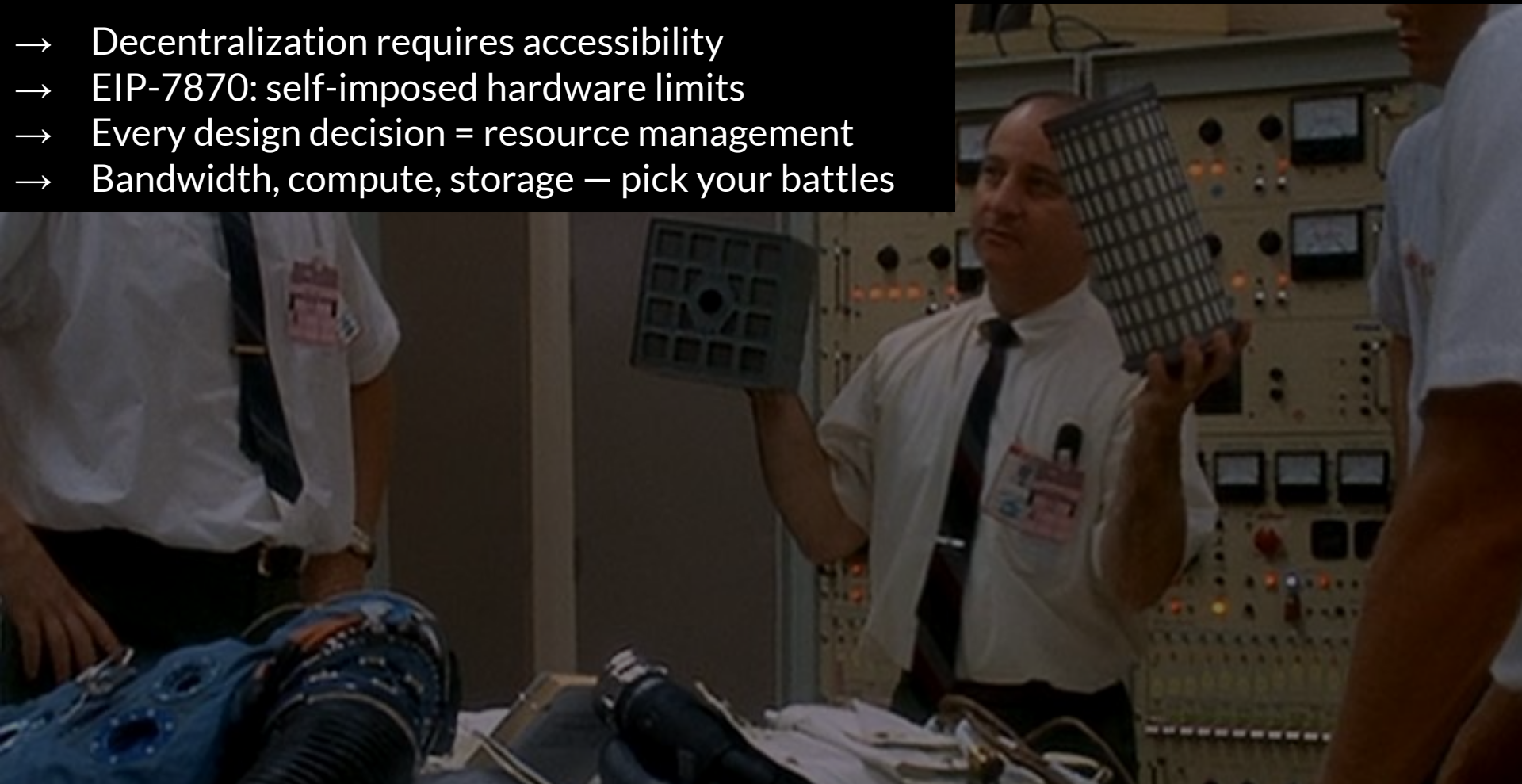
RESEARCH+SPECS+TESTING+COORDINATION

→ EF doesn't build a CL client
→ We do research, write specs, coordinate testing
→ Client teams do implementation
→ My job: connect the dots across all of it



L1——ENGINEERING UNDER CONSTRAINTS

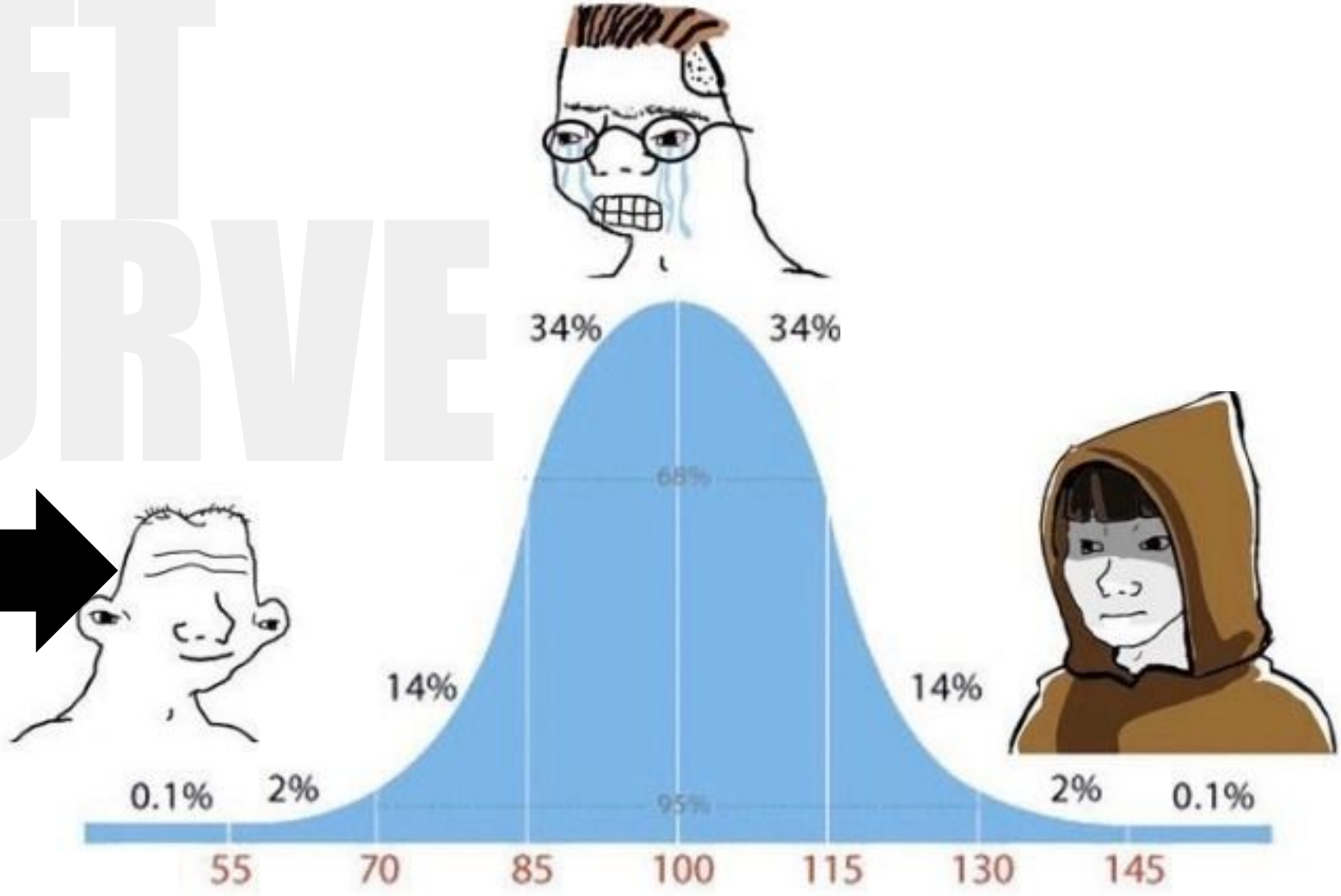
→ Decentralization requires accessibility
→ EIP-7870: self-imposed hardware limits
→ Every design decision = resource management
→ Bandwidth, compute, storage — pick your battles




Part 2
QUANTUM COMPUTING 101
→ Quantum Computing 101 — why this threat is real and inevitable

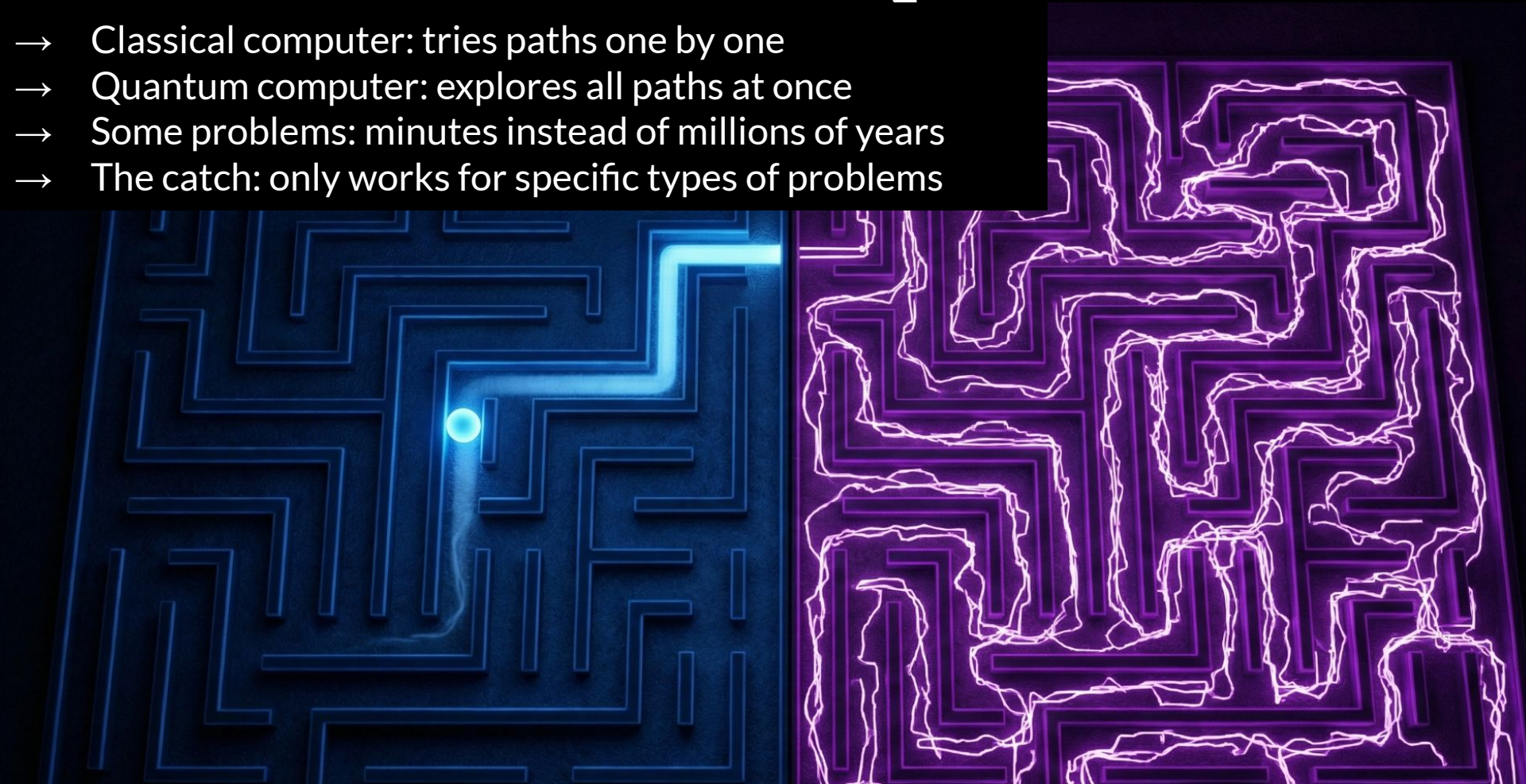
LEFT CURVE

you are here



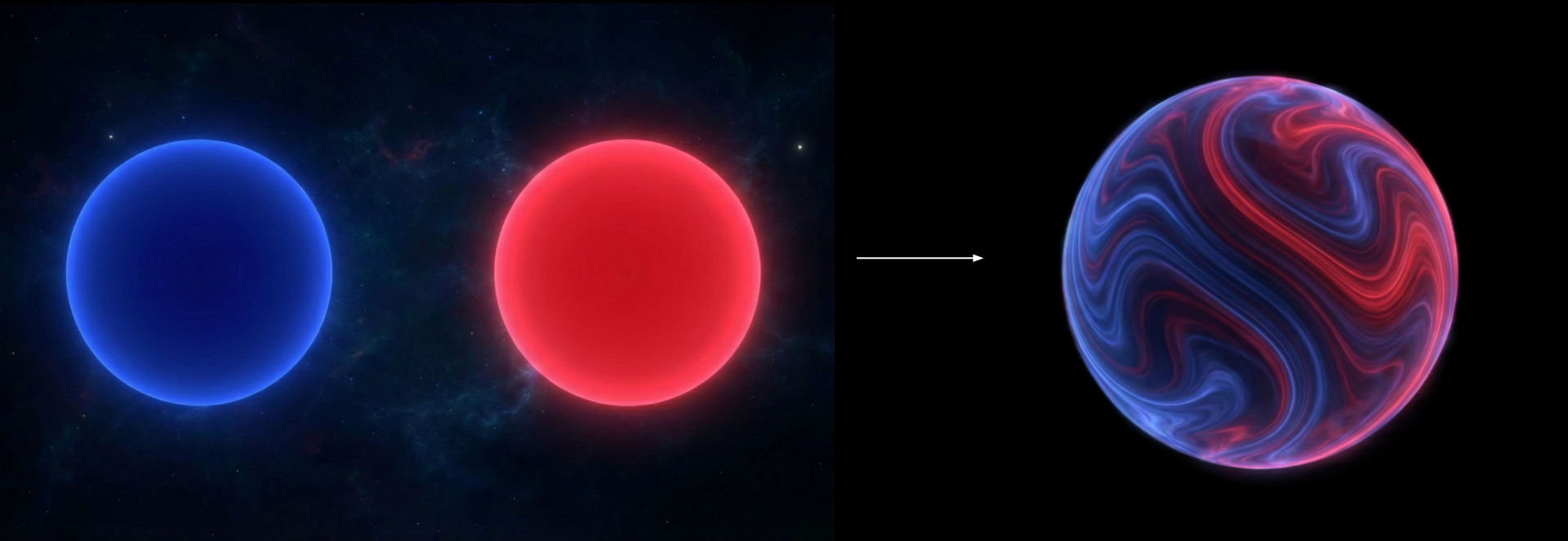
THE MAZE: CLASSICAL VS. QUANTUM

→ Classical computer: tries paths one by one
→ Quantum computer: explores all paths at once
→ Some problems: minutes instead of millions of years
→ The catch: only works for specific types of problems



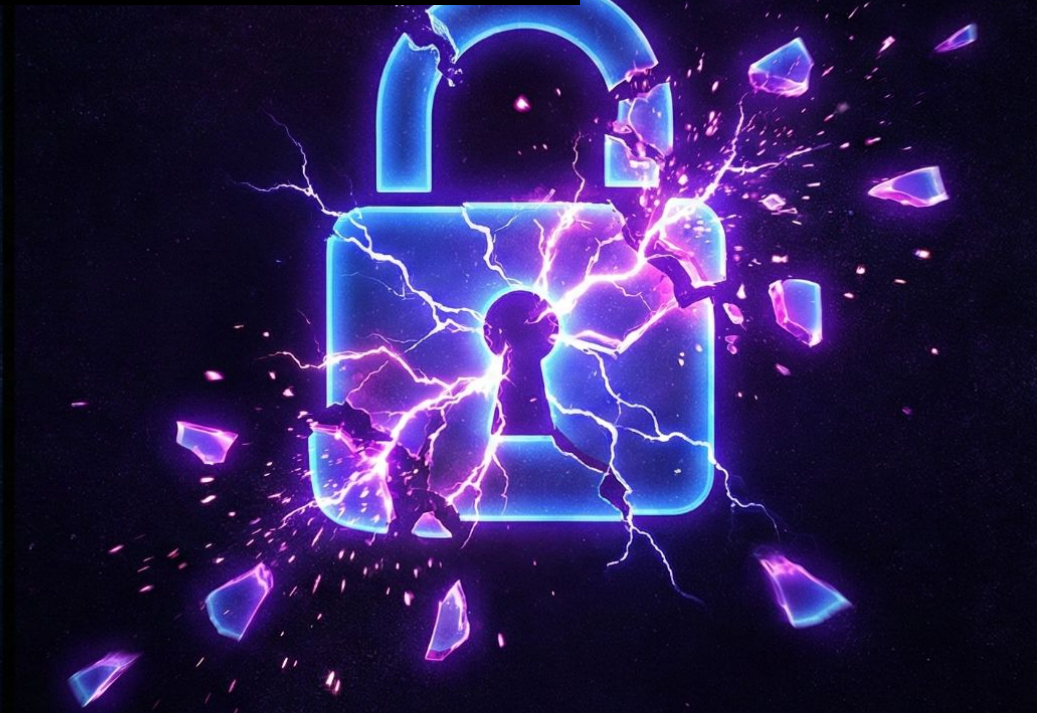
QUIBIT AND SUPERPOSITION

→ Classical bit: 0 OR 1 (switch on or off)
→ Qubit: 0 AND 1 simultaneously
→ When measured, it "picks” or “collapses" to one state
→ Weird? Yes. Real? Also yes.



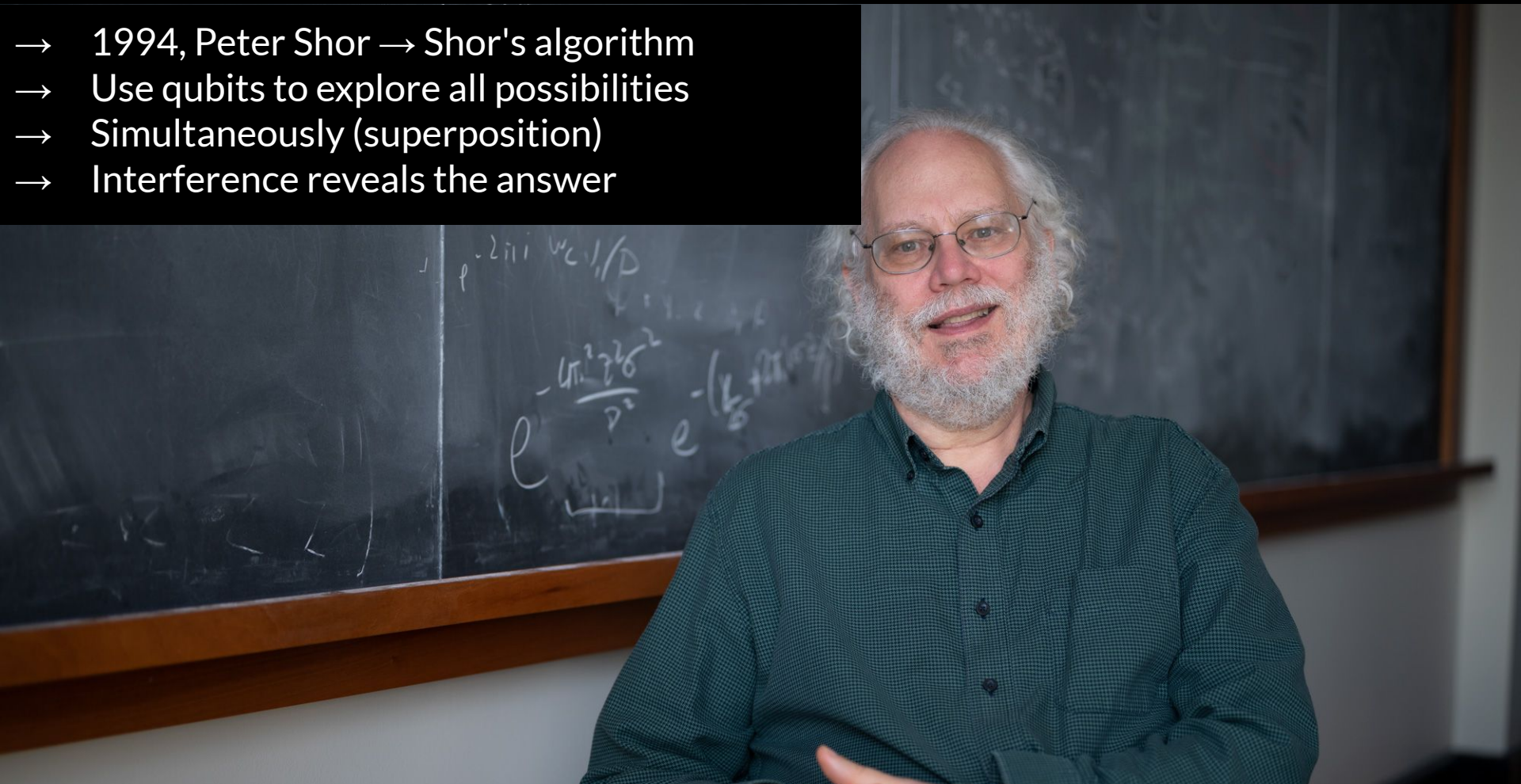
CRACKING PUBLIC KEY CRYPTOGRAPHY

- → Public key crypto = math problems that are hard to reverse
- → Example: 17 × 31 = 527 (easy) → 527 = ? × ? (hard)
- → Classical computers: check possibilities one by one
- → Hard problem becomes easy problem

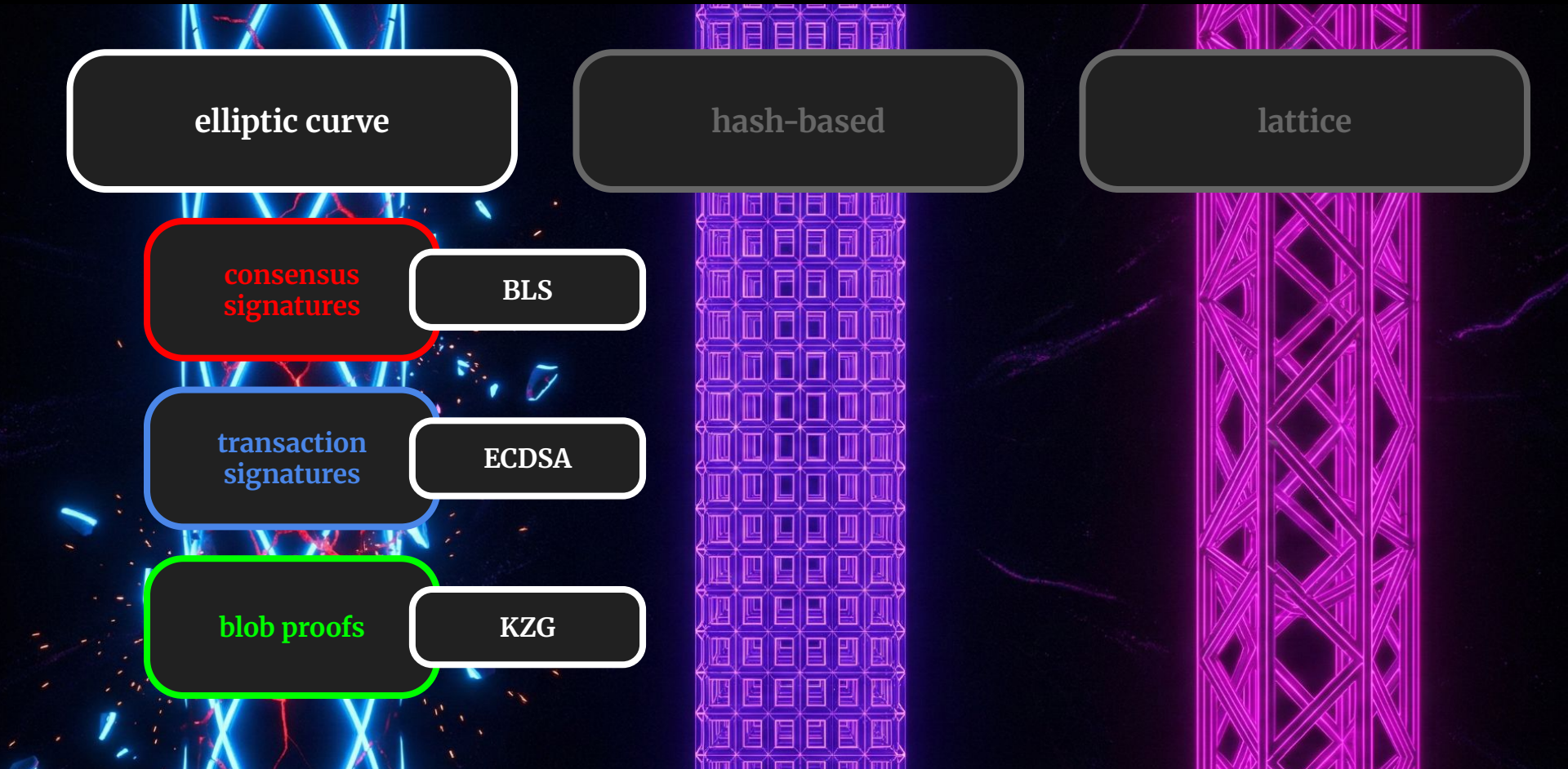


SHOR'S ALGORITHM

→ 1994, Peter Shor → Shor's algorithm
→ Use qubits to explore all possibilities
→ Simultaneously (superposition)
→ Interference reveals the answer



WHAT BREAKS VS. WHAT DOESN'T

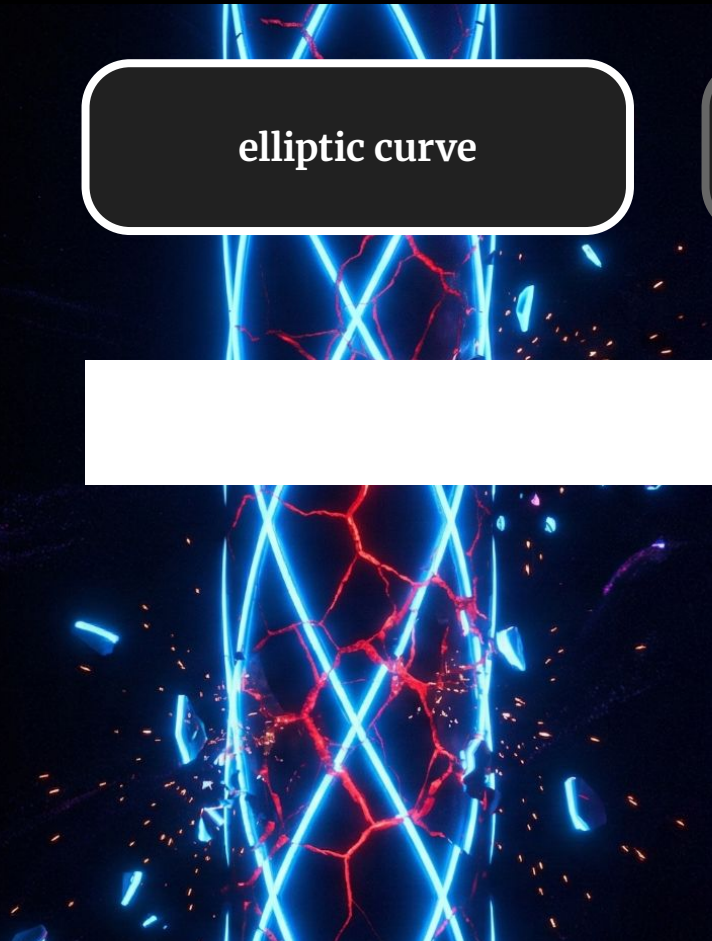


WHAT BREAKS VS. WHAT DOESN'T

elliptic curve

hash-based

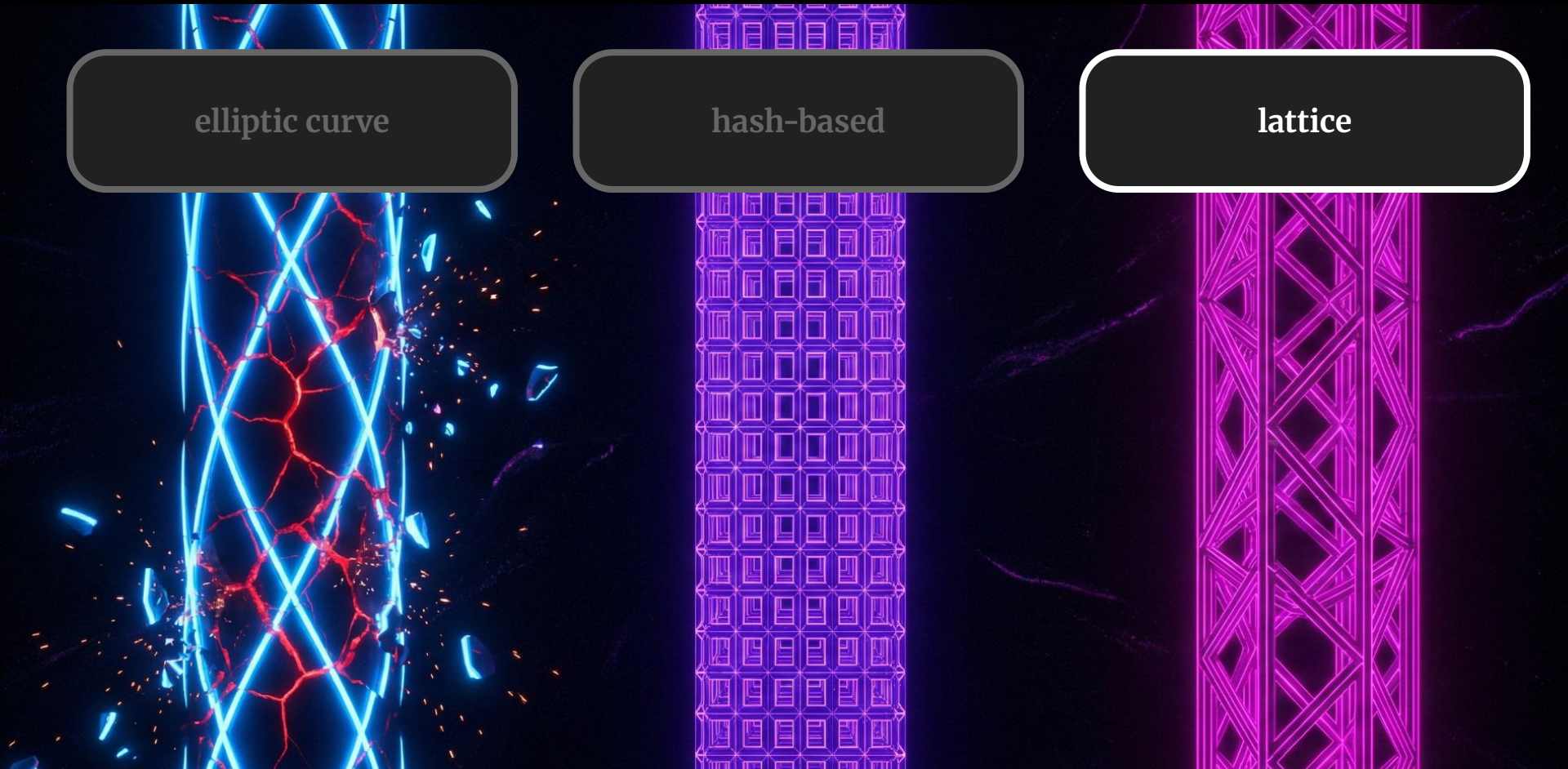
lattice



WHY CHOOSE ECC IF IT BREAKS?

- Tiny (96 bytes)
- Aggregatable (10k sigs, still 96 bytes)
- Decades of cryptanalysis

WHAT BREAKS VS. WHAT DOESN'T



WHAT BREAKS VS. WHAT DOESN'T

Part 3

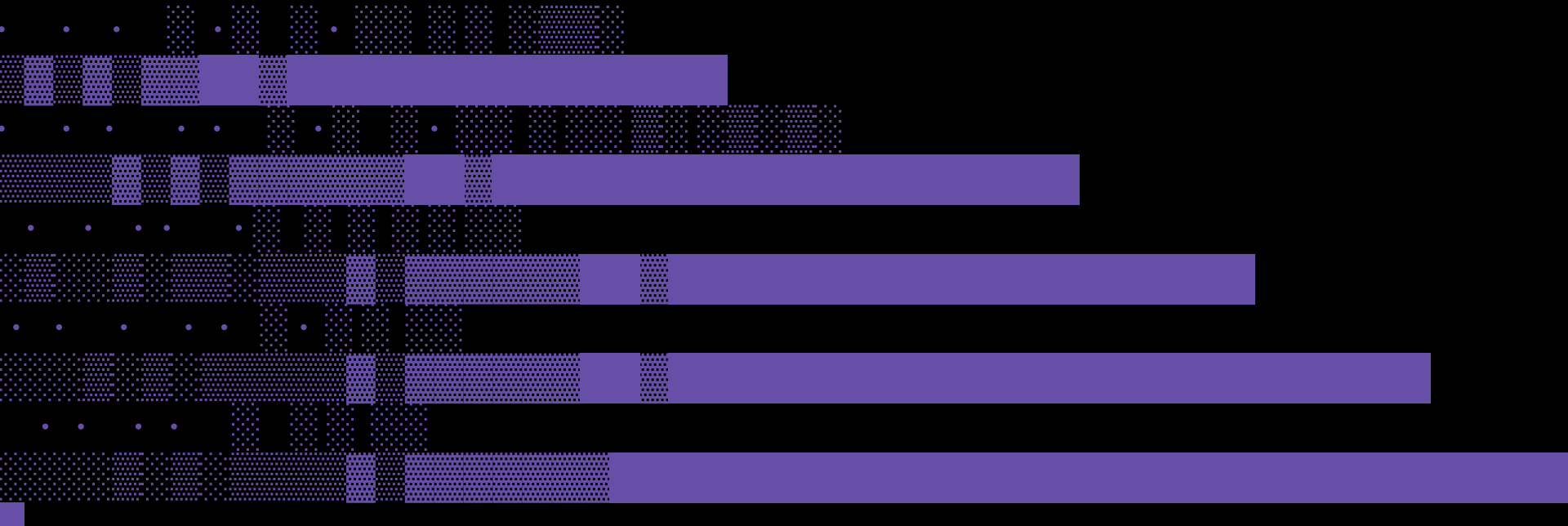
THE SIZE PROBLEM

→ The size problem — why post-quantum is harder than it sounds

THE SIZE EXPLOSION

→ BLS signature → 96 bytes

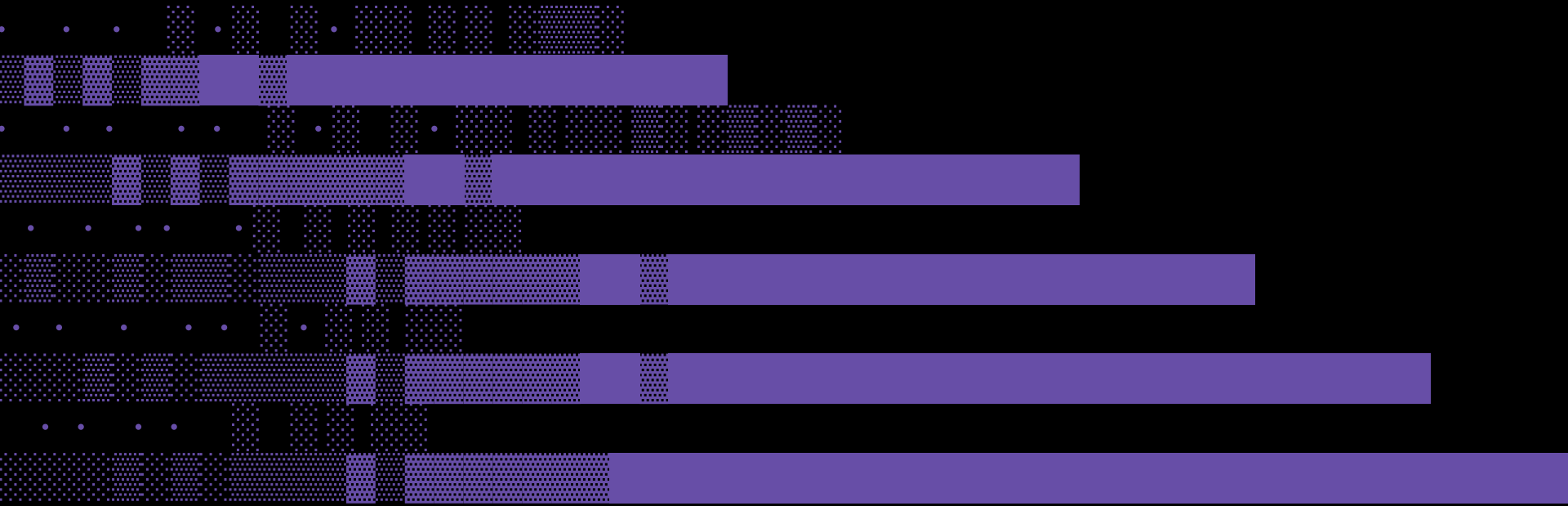
→ BLS aggregated (10k) → 96 bytes(!)



THE SIZE EXPLOSION

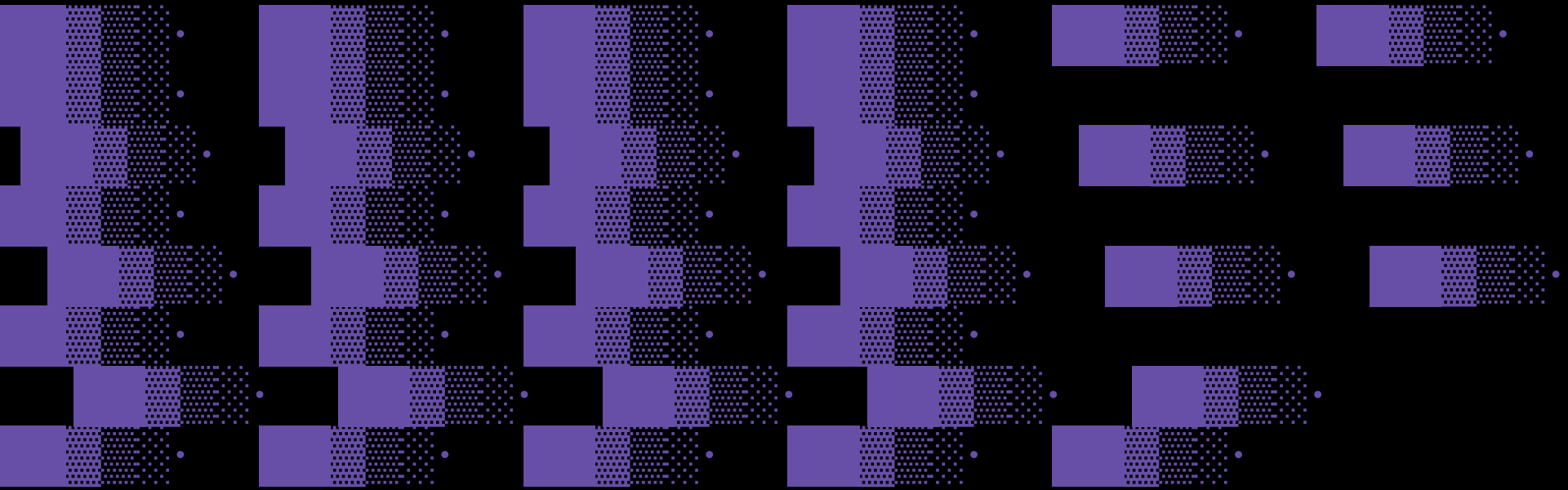
→ BLS signature → 96 bytes
→ BLS aggregated (10k) → 96 bytes(!)

→ PQ sig → 3,000 bytes
→ PQ sig agg (10k) → 30 MB per slot!



THE CASCADE OF CONSTRAINTS

- → Bigger signatures → more bandwidth
  - More bandwidth → fewer home validators
    - Fewer home validators → less decentralization
      - Less decentralization → weaker security guarantees
        - One change cascades through everything



THE FOUR REQUIREMENTS

→ Quantum-resistant — won't break when Q-day arrives
→ Fast to verify — consensus can't slow down
→ Compact — can't break bandwidth budgets
→ Aggregatable — must combine thousands efficiently

Part 4

THE SOLUTION

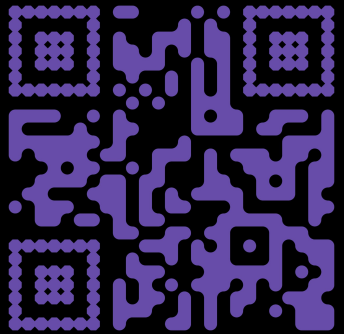
→ The solution — leanMultisig, and the full stack

LEANSIG + LEANMULTISIG

leanSig	leanMultisig
Hash-based signatures scheme (XMSS variant)	SNARK aggregation engine
Quantum-resistant (only uses hash functions)	Proves “I verified N valid signatures”
~3,000 bytes per signature	10,000 signatures → ~300 KB proof (100x compression)

leanMultisig stack

A Ream study group session



THE FIVE STEPS OF LEANMULTISIG

step	description
Program	Write a program for what you want to prove using custom DSL (leanDSL)
Compile	Translate the program to a minimal instruction set for a VM (leanISA)
Execute	Run the compiled program with signatures, get execution trace
Prove	Generate a zk-Proof proving the correctness of the execution trace
Verify	Anyone can verify the zk-Proof without re-execution

minimal VM
(4x1)

THE FULL LEAN STACK

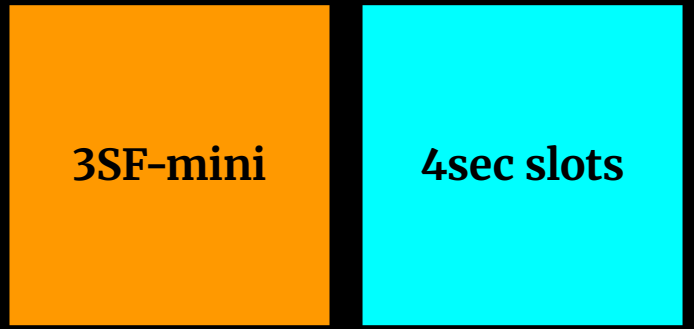
component	purpose
leanSpec	Python specification (the rulebook) + test vectors + pyclient
leanSig	Hash-based signature library
leanDSL	Language for writing provable programs
leanISA	Minimal instruction set (4 ops + 1 precompile)
leanVM	Minimal zkVM that executes leanISA
leanMultisig	Aggregation logic (written in leanDSL)
lean-quickstart	Multi-node local devnet tool
leanMetrics	Observability across lean clients

10 CLIENT TEAMS ENGAGED

team	language	status
Zeam	Zig	Interoping on devnets
Ream	Rust	Interoping on devnets
Qlean	C++	Interoping on devnets
Lantern	C	Interoping on devnets
Ethlambda	Rust	Interoping on devnets
Geam	Go	In development
Lighthouse	Rust	In development
Grandine	Rust	In development
Nimbus	Nim	In development
Prysm	Go	soonTM

PQ-DEVNET

devnet	key feature	status
pq-devnet-0	leanSpec, multi-client p2p	✅ sept 2025
pq-devnet-1	leanSig (agg by concatenation)	✅ nov 2025
pq-devnet-2	leanMultisig (linear aggregation)	✅ jan 2026
pq-devnet-3	Implement 3SF-ish consensus	soonTM
pq-devnet-4	leanVM (recursive aggregation)	soonTM + 1
pq-devnet-5	fast finality-ish finality gadget	soonTM + 2



Part 5

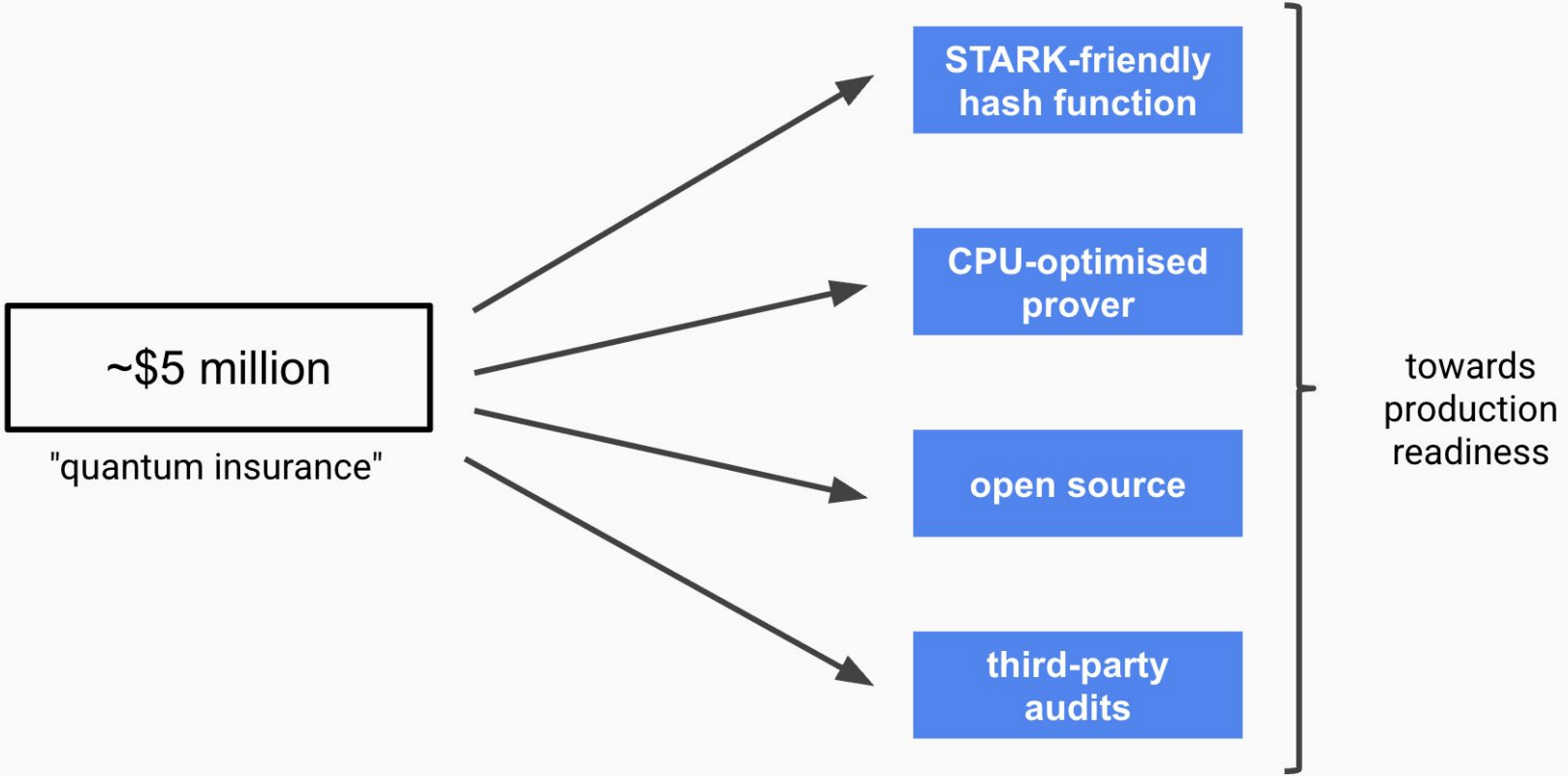
THE EFFORT

→ The effort — 8+ years of research and building, $30M+ invested

THIS DIDN'T HAPPEN OVERNIGHT

Ethereum Foundation grant (July 2018)

2018



THIS DIDN'T HAPPEN OVERNIGHT

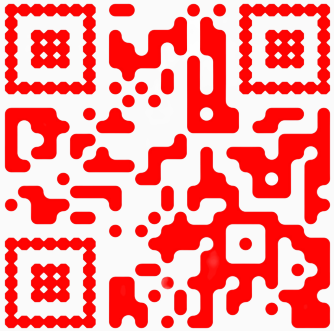
post quantum narrative

2019

> What's your vision for Eth 3.0?

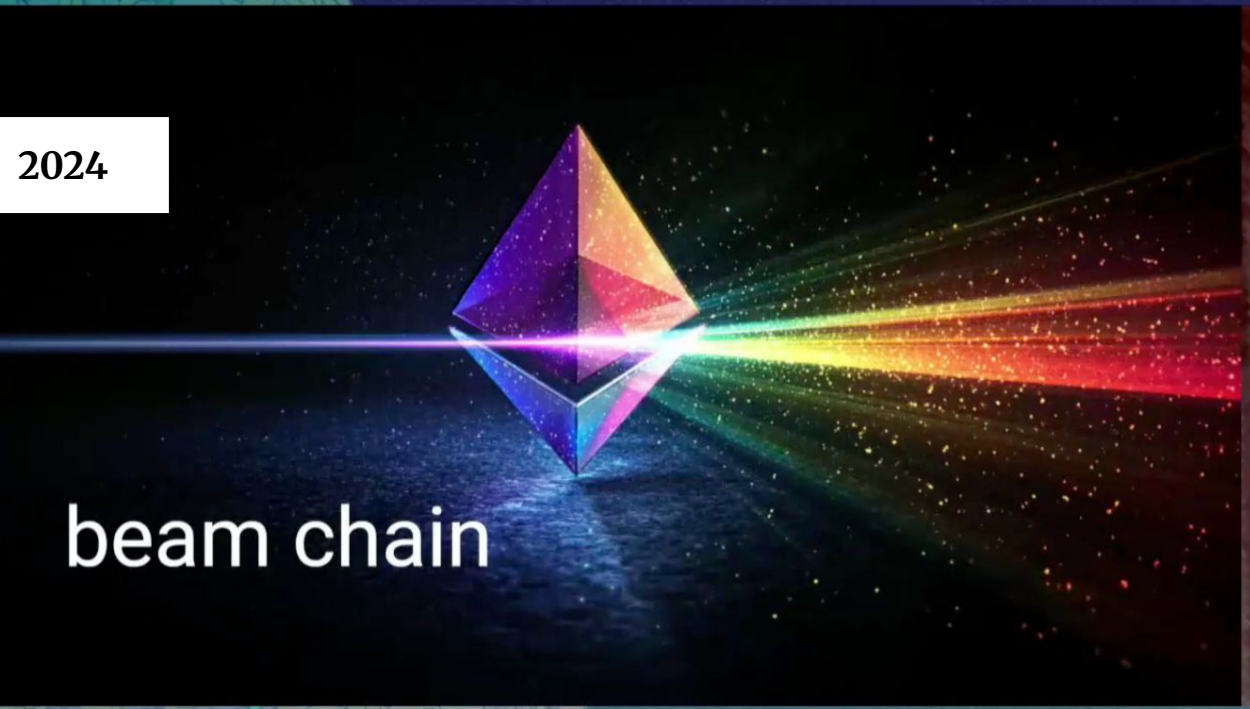
"**STARKs, STARKs and lots of STARKs.**"—Vitalik, Jan 2019

- **flexibility**
  - one tool to rule them all
- **lean and resilient crypto**
  - consolidation of assumptions
  - hash functions only
  - Lindy effect
- **performance**
  - relatively fast prover
  - data is cheap™



THIS DIDN'T HAPPEN OVERNIGHT

2024



THIS DIDN'T HAPPEN OVERNIGHT

2019—present

Poseidon2: A Faster Version of the Poseidon Hash Function

Lorenzo Grassi[1,2], Dmitry Khovratovich[3], and Markus Schofnegger[4]

[1] Ponos Technology (Switzerland)
[2] Ruhr University Bochum (Germany)
[3] Ethereum Foundation (Luxembourg)
[4] Horizen Labs (United States)
lorenzo@ponos.technology, khovratovich@gmail.com,
mschofnegger@horizenlabs.io

Abstract. Zero-knowledge proof systems for computational integrity have seen a rise in popularity in the last couple of years. One of the results of this development is the ongoing effort in designing so-called *arithmetization-friendly* hash functions in order to make these proofs more efficient. One of these new hash functions, Poseidon, is extensively used in this context, also thanks to being one of the first constructions tailored towards this use case. Many of the design principles of Poseidon have proven to be efficient and were later used in other primitives, yet parts of the construction have shown to be expensive in real-word scenarios.

In this paper, we propose an optimized version of Poseidon, called Poseidon2. The two versions differ in two crucial points. First, Poseidon is a sponge hash function, while Poseidon2 can be either a sponge or a

Poseidon Cryptanalysis

Scrutinizing Poseidon for Good

Running Team

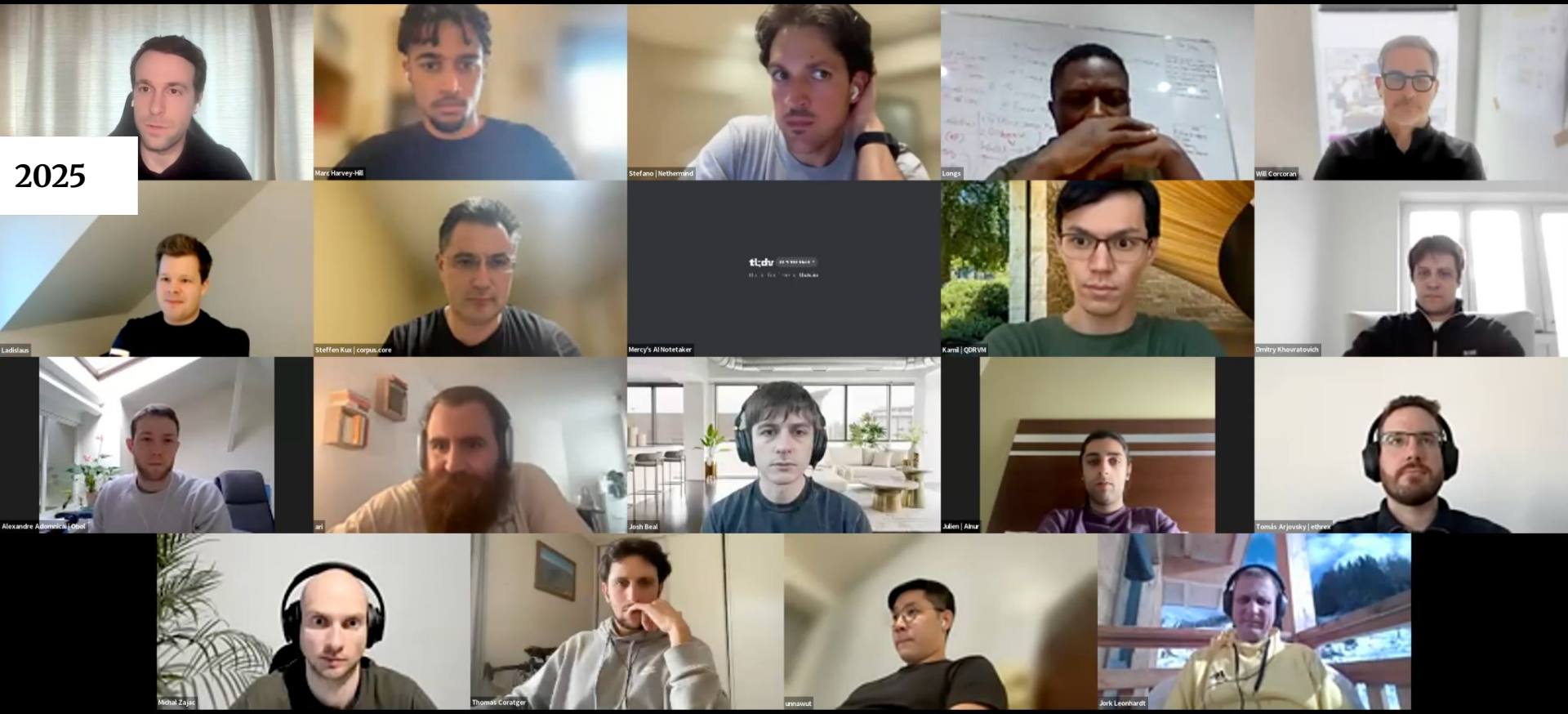
The project is run by the Ethereum Foundation Poseidon Group (EFPG: poseidon@ethereum.org):

- George Kadianakis
- Dmitry Khovratovich
- Antonio Sanso

The **Advisory Board** oversees key decisions and announcements made by EFPG, with members serving in an unpaid capacity:

- Jean-Philippe Aumasson (Taurus)
- Eli Ben-Sasson (Starknet)
- Daira-Emma Hopwood (ZCash)
- Daniel Lubarov (PolygonZero)
- Ron Rothblum (Succinct)

THIS DIDN'T HAPPEN OVERNIGHT



THIS DIDN'T HAPPEN OVERNIGHT

2025

THIS DIDN'T HAPPEN OVERNIGHT

2025

THIS DIDN'T HAPPEN OVERNIGHT

THIS DIDN'T HAPPEN OVERNIGHT

Justin Drake ✓
@drakefjustin

Today marks an inflection in the Ethereum Foundation's long-term rategy.

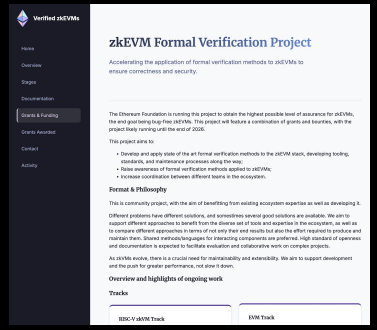
2026

ed a new Post Quantum (PQ) team, led by the brilliant Thomas Coratger (@tcoratger). Joining him is Emile, one of the world-class talents behind leanVM. leanVM is the cryptographic cornerstone of our entire post-quantum strategy.

After years of quiet R&D, EF management has officially declared PQ security a top strategic priority. Our journey began in 2019, with the "Eth3.0 Quar
2024, PQ has
engineering b
phenomenal.

It's now 202

→ **PQ ACD**: A
Devs PQ tran
user-facing s
abstraction, and longer-term transaction signature aggregation with



→ **PQ foundations**: Today we are announcing a $1M Poseidon Prize to harden the Poseidon hash function. We are betting big on hash-based cryptography to enjoy the strongest and leanest cryptographic foundations. Check out our other $1M PQ initiative, the Proximity Prize.
→ **PQ devnets**: Multi-client PQ consensus devnets are live! Shoutout to pioneers @zeamETH, @ReamLabs, @PierTwo_com, @geanclient, @ethlambda_lean, as well as established consensus teams Lighthouse, Grandine, and soon Prysm. This incredible teamwork is coordinated by @corcoranwill via weekly PQ interop calls.
→ **PQ workshops**: Building on last year's PQ workshop in Cambridge (see photo), the EF is hosting another 3-day PQ event in October. Top experts from around the world will convene. In addition, a PQ day is set for March 29 in Cannes just ahead of EthCC.

also preparing material for enterprises and nation-states. Finally,

THIS DIDN'T HAPPEN OVERNIGHT

EthCC PQ: www.luma.com/beast_mode

EthCC zkVM: www.luma.com/fort_mode

cambridge PQ retreat 2.0: oct 2026

Part 6

INDUSTRY & L2 IMPLICATIONS

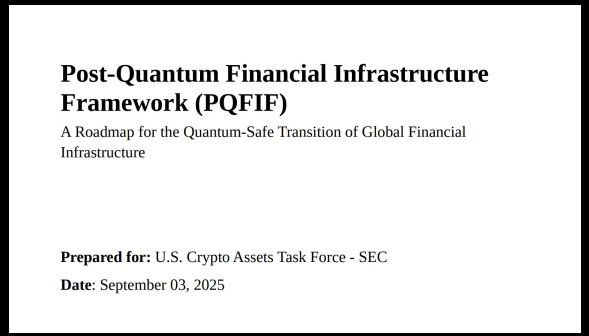
→ Why this is your problem too

ETHEREUM—SET THE INDUSTRY STANDARD

→ Every blockchain faces this exact same problem
→ Hash-based signature aggregation is non-negotiable for security + performance
→ EF is the only entity seriously working on aggregation at scale
→ If we succeed → de facto industry standard
→ Just like Bitcoin's ECDSA became the default

INSTITUTIONS ARE WAKING UP

→ Citi: major quantum security report published
→ US Government: PQC-compliant by 2027 (new), 2030 (existing)
→ Bank of Israel: quantum readiness mandates
→ HSBC: testing quantum key distribution



"FULL LIFT AND SHIFT"

L2 component	why it's potentially vulnerable
Bridge contract	Sign repeatedly → exposed
Admin / upgrade keys	Used once → exposed
Sequencer signing	ECDSA → breakable
Validity proofs	May use vulnerable verification

"Every protocol must migrate. Every smart contract must be redeployed. Every single asset must move."

— Alex Prudin, Project 11

PROJECT ELEVEN

Securing digital assets for the post-quantum era

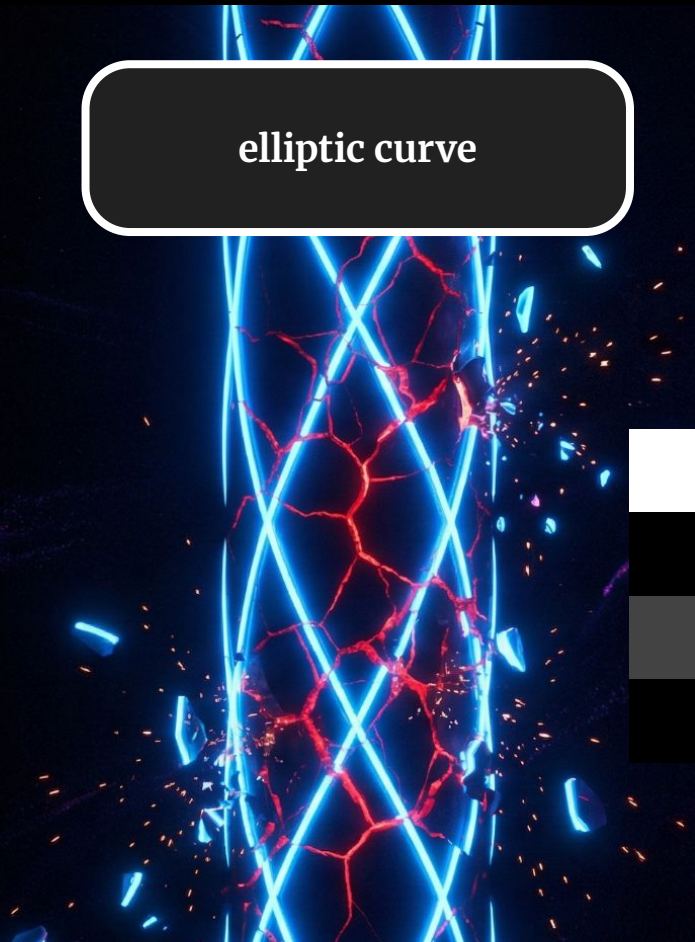
fin

THANK YOU!

→ @corcoranwill

→ www.leanroadmap.com

WHAT BREAKS VS. WHAT DOESN'T



elliptic curve

hash-based

lattice

type	why it breaks / doesn't
Elliptic curve	Has periodic structure → Shor's finds the pattern
Hash-based	No structure → nothing to find
Lattice	Has structure, but not periodic → Shor's doesn't apply

WHAT BREAKS VS. WHAT DOESN'T

elliptic curve

hash-based

lattice

layer	primitive	purpose
Consensus	BLS	Validator signatures
Execution	ECDSA	Transaction signatures
Data	KZG	Blob commitments

Why we chose ECC:

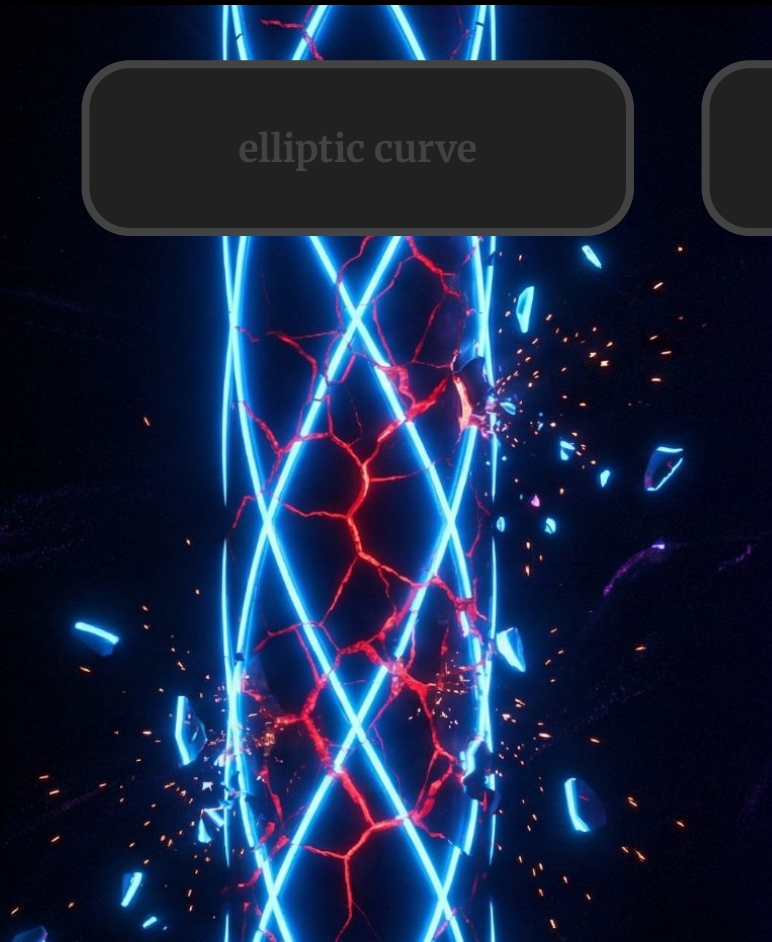
- Tiny (96 bytes)
- Aggregatable (10k sigs, still 96 bytes)
- Decades of cryptanalysis

WHAT BREAKS VS. WHAT DOESN'T

elliptic curve

hash-based

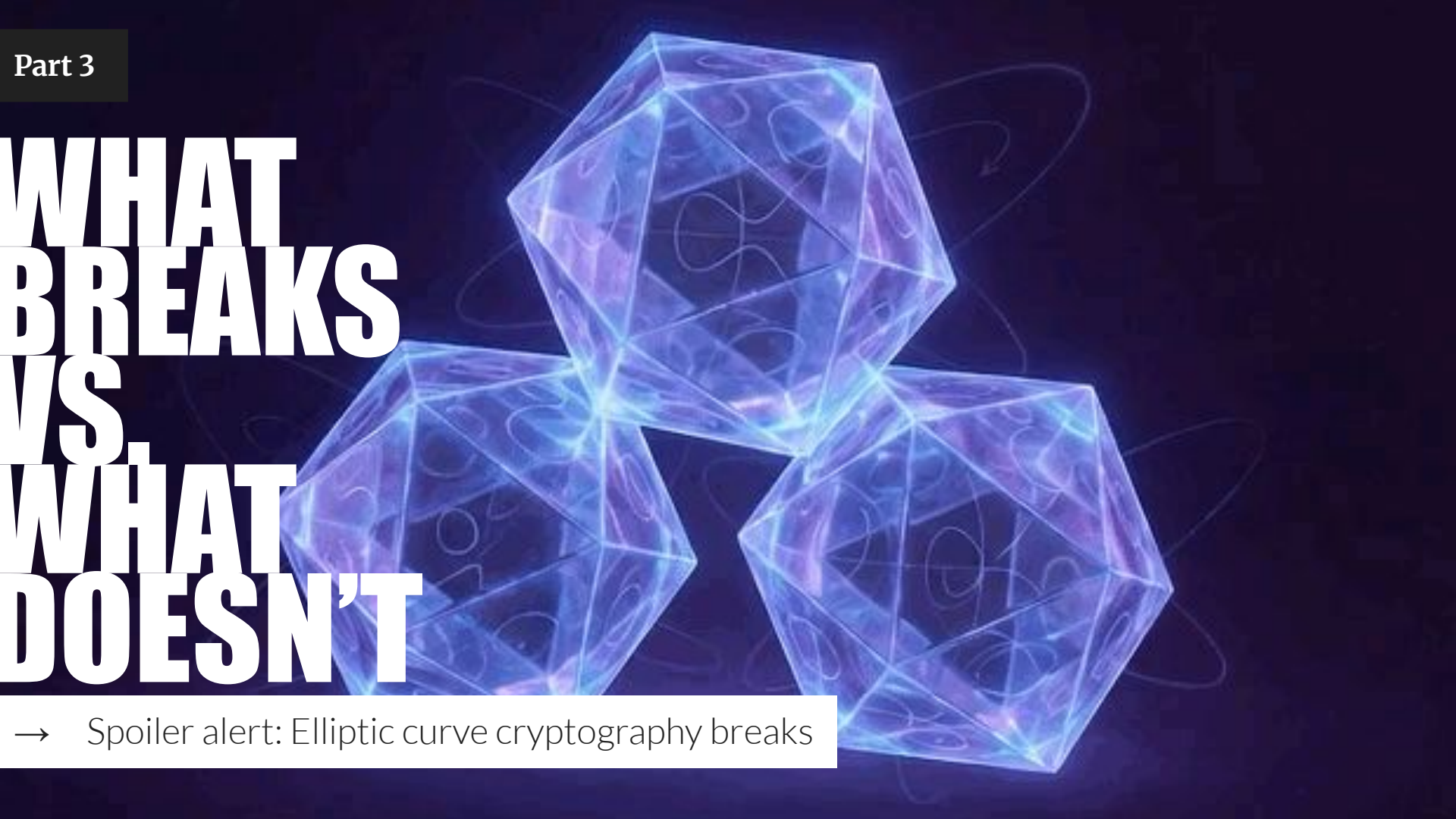
lattice



Lattice assessment for Ethereum
✅ Quantum-safe (Shor's doesn't apply)
✅ NIST standardized
❌ No strong aggregation candidate

Part 3

WHAT BREAKS VS. WHAT DOESN'T



→ Spoiler alert: Elliptic curve cryptography breaks