

# **Coordinating Post-Quantum Migration in Decentralised Systems**

**An independent research proposal using Ethereum as a case study**

Dr Hui Gong

University College London

Cambridge Forum on Institutions Under Technological Change

Downing College, 10 October 2026

# Public signals informing this proposal

- **Jan 2026** Ethereum Foundation forms a dedicated post-quantum team.
- **Feb 2026** Vitalik identifies four areas of Ethereum requiring PQ upgrades.
- **7 Sep 2026** EF Protocol publishes a December 2029 L1 planning target.
- **THIS WEEK**
- **6 Oct** Singapore: Vitalik discusses AI agents and the security challenges they create.
- **7 Oct** Justin Drake calls for calm planning for a possible “bunker mode”.
- **7–8 Oct** Vitalik urges serious attention to AI-driven cryptographic risk and careful migration.

Published context, not a commitment by the speaker. No public evidence shows ECDSA is broken today.

Sources: [ethereum.org](https://ethereum.org); EF Protocol (7 Sep); Singapore speech, trans. Wu Blockchain/PANews (6 Oct); The Block (7–8 Oct).

# ACHILLES' HEEL



**My focus is the coordination gap in post-quantum migration.**

Secure algorithms still need adoption across actors that no one can compel.

# Three clocks determine whether migration succeeds

**EXPOSURE** $T_D$ 

How long data, keys and control rights  
must remain secure

**MIGRATION** $T_M$ 

Discovery, standards, implementation,  
testing and adoption

**BREAKTHROUGH** $T_Q$ 

Time until relevant cryptanalysis  
becomes deployable

$$T_D + T_M > T_Q \quad \Rightarrow \quad \text{act before certainty}$$

AI matters here because it can widen the uncertainty around  $T_Q$  and compress the time available for  $T_M$ .

Adapted from Mosca's migration-risk inequality; interpretation for open blockchain systems.

# PQC is already an implementation problem

**2024**

NIST finalised ML-KEM, ML-DSA  
and SLH-DSA

$\leq 1,200$

Logical qubits in Google's 2026  
secp256k1 estimate

**Dec 2029**

EF Protocol's published L1 planning  
target

Standards exist



System designs lag



Adoption  
takes years

Sources: NIST (13 Aug 2024); Babbush et al., PRX Quantum 7 (2026); Ethereum Foundation Protocol priorities (7 Sep 2026).

# Why a public chain is harder to migrate

## No central switch

Protocol developers can ship options; they cannot compel every holder, validator, bridge or application to use them.

## Permanent public evidence

Transactions expose keys and dependencies that cannot be withdrawn from the historical ledger.

## Composability creates spillovers

One vulnerable admin key can govern contracts, bridges, oracles and downstream collateral.

## Dormancy is a governance problem

Inactive owners may not migrate. Lost keys may leave reachable value if no secure recovery route exists.

**Migration is a collective-action problem under hard capacity constraints.**

# Proposed case-study scope using Ethereum

## Execution

ECDSA accounts

Many holders.  
Sending a transaction exposes the public key.

## Consensus

BLS signatures

PQ signatures are larger. Efficient aggregation remains essential.

## Data

KZG commitments

No drop-in PQ replacement at Ethereum scale.

## Applications

EC-based proofs

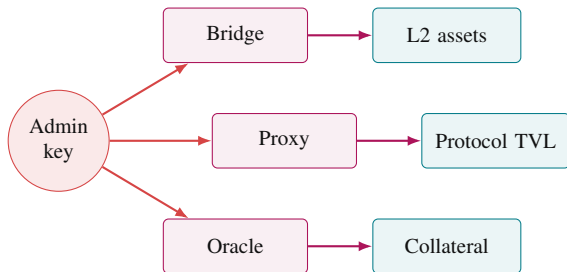
Rollups and privacy systems rely on different assumptions.

### CASE STUDY LOGIC

Open data + public roadmap + visible dependencies

Source: ethereum.org, "Post-quantum cryptography on Ethereum," updated 8 Sep 2026.

# Proposed measurement of systemic exposure



Illustrative dependency map. The proposed measurement is a research design, not an empirical result.

## Balance asks:

How much does this account hold?

## Systemic exposure asks:

How much value can fail when this key fails?

## Proposed measurement:

Connect exposed keys to downstream loss, accounting for access rules and safeguards.

# Proposed migration priority based on systemic exposure

## Baseline balance ranking

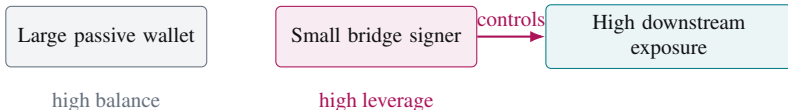
$$\text{priority}_i \propto \text{balance}_i$$

Misses control rights, dependencies and correlated failure.

## Proposed systemic ranking

$$\text{priority}_i \propto \underbrace{p_i}_{\text{exposure}} \times \underbrace{L_i}_{\text{direct loss}} + \underbrace{S_i}_{\text{spillover}}$$

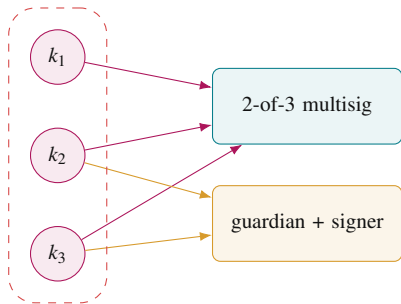
Tests which migrations reduce the most network risk per unit of capacity.



Conceptual priority rule for evaluation; not an Ethereum policy or a validated scheduling result.

# Proposed access model using a threshold hypergraph

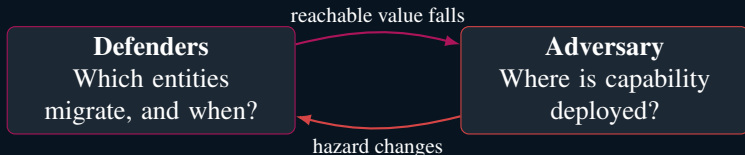
access hyperedge



- Some keys are **substitutes**: any two can authorise.
- Others are **complements**: both roles are required.
- A key's value depends on the access sets in which it participates.
- Mixed threshold logic can invalidate greedy guarantees; test exact integer optimisation on the mapped sample.

Illustrative access structures for the proposed model. Feasible exact solution depends on the mapped problem's scale.

# Proposed model of migration and attack incentives



## Endogenous hazard

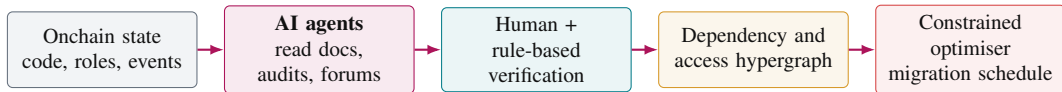
An attack capability may be developed elsewhere, then deployed against the most attractive remaining target.

## Dormant-value floor

Lost keys without secure recovery may leave reachable value. If this floor exceeds the attack threshold, deterrence may be impossible.

**Research hypothesis: migration elsewhere may redirect attack incentives.**

## Proposed role of AI agents in evidence collection



### Agents are useful where

Meaning is dispersed across natural-language documentation, audit reports and governance threads.

### Agents should not replace

Deterministic queries, graph construction, exact optimisation, security review or legitimate governance.

# Proposed scheduling objective and constraints

## Illustrative objective

$$\min_{x_{it}} \sum_t h_t \mathbb{E}[L(G_t)] + \lambda \sum_{i,t} c_{it} x_{it}$$

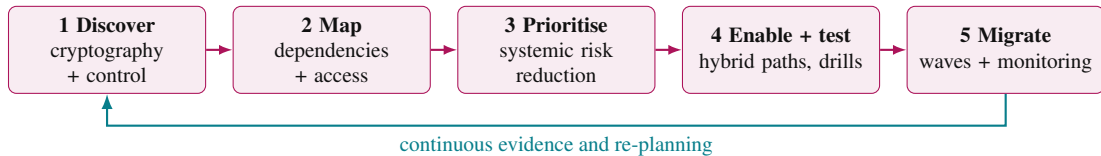
- $x_{it} = 1$ : entity  $i$  migrates in period  $t$
- $G_t$ : vulnerable dependency hypergraph at  $t$
- $h_t$ : scenario-dependent attack hazard
- $c_{it}$ : migration and operational cost

Proposed output: a decision aid with auditable assumptions. Humans retain authority over migration.

## Constraints that matter

- BLOCKSPACE** signature size and verification
- ENGINEERING** wallet, client and audit capacity
- DEPENDENCY** migrate prerequisites first
- ACCESS** thresholds and dormant owners
- GOVERNANCE** consent, appeals and legitimacy

# Proposed operating model for ecosystem migration



## Technical readiness

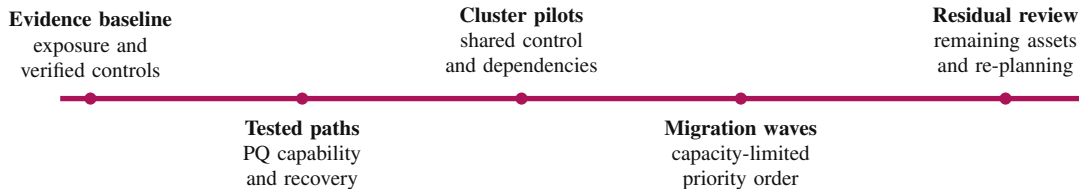
PQ verification, account agility, testnets, recovery routes and emergency modes.

## Coordination readiness

Ownership, incentives, disclosure, capacity allocation and treatment of non-migrating assets.

Hui Gong's independent proposal for evaluation. This model does not specify an official Ethereum upgrade schedule.

# My proposed migration sequence for the case study



## Conditional progression

Proceed after evidence, secure paths and capacity pass agreed checks. Pilots require available protocol capabilities.

## Ecosystem agreement

Participation, incentives and non-migrating assets require legitimate decisions. The proposal gives no power to compel migration.

Hui Gong's independent research proposal. Illustrative sequence with no official Ethereum endorsement or implementation commitment.

# Proposed evaluation with Ethereum data

## Build the evidence base

- exposed-account and key-reuse data
- proxy, admin, bridge and oracle permissions
- multisig and threshold access structures
- audit reports and governance evidence
- migration capacity and cost scenarios

## Test four hypotheses

1. systemic and balance rankings differ;
2. dependency-aware schedules reduce expected spillover;
3. agent-assisted extraction improves coverage;
4. dormant-value bounds reveal deterrence and indeterminate regimes.

**Planned Ethereum case study; generalisation remains to be tested.**

# Post-quantum security is a migration outcome

not an algorithm property

- 1 The clock starts before Q-day because migration is slow and exposure persists.
- 2 I propose priorities based on systemic dependency and control alongside balance.
- 3 My proposed architecture combines agent-assisted evidence with human authority.

# Selected sources and scope of this proposal

- Ethereum Foundation, *EF Protocol: Current and Emerging Priorities*, 7 Sep 2026.
- ethereum.org, *Post-quantum cryptography on Ethereum*, updated 8 Sep 2026.
- Babbush et al., *Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities*, PRX Quantum 7 (2026).
- NIST, *Approval of Three FIPS for Post-Quantum Cryptography*, 13 Aug 2024.
- OKX, *OKX Now Recap*, Singapore, 6 Oct 2026.
- Vitalik Buterin, *Singapore remarks*, translated transcript by Wu Blockchain/PANews, 6 Oct 2026.
- The Block, *Ethereum researcher calls for “bunker mode” planning*, 7 Oct 2026.
- The Block, *Vitalik warns against hasty wallet migrations*, 8 Oct 2026.

## Independent research proposal

Published Ethereum plans provide context. The coordination model and migration sequence are my proposals, with no official Ethereum mandate or endorsement. AI-related comments do not establish a cryptographic break.