Post-Quantum Cryptography Migration on DLTs

Deployment, Agility & Governance

Blockchain Governance Initiative Network

BGIN – Mitchell Travers & Shin'ichiro Matsuo

Global Digital Collaboration | Geneva | 2–3 September 2026

Post-Quantum Cryptography Migration on DLTs

Wallets and credentials rely on long-lived cryptographic trust. NIST-standardized post-quantum cryptography is available. The work in this room is deployment, crypto agility, and governance — not a new algorithm contest.

Co-organizers

ISO, Blockchain Group: BGIN, Blockchain Bundesverband e.V, Ethereum Climate Platform, LNet, Linux Foundation Group: OpenWallet, Trust Over IP, LF Decentralized Trust

The Job Is Not to Pick Another Primitive

First PQC standards are in place (ML-KEM, ML-DSA, SLH-DSA). Re-running a competition inside this breakout would waste the hour.

What still has no agreed playbook for public ledgers, wallets, and credentials:

- How to stage a hybrid then a cutover when every node must agree on validity rules.
- How to keep verifying old signatures for as long as funds and archives remain live.
- How to rotate keys and addresses without stranding dormant accounts.
- How to tell a genuine PQ-ready stack from a screenshot.

🔗 **Takeaway:** Treat PQC as a multi-year systems and governance program, not a weekend library swap.

Why This Stack Does Not Migrate Like TLS

Enterprise PKI / TLS	Public DLT / wallets
An operator can force a cutover	No single party can force consensus
Cipher suites can be negotiated per session	Validity rules are global and sticky
Certificates expire on a known clock	On-chain signatures must stay verifiable for decades
Harvest-now, decrypt-later is mainly archival	Public keys often sit in the clear on-chain
Evidence lives in a vendor report	"PQ-ready" claims need comparable measurement

🔗 **Takeaway:** A TLS playbook fails on three axes at once: decentralized upgrades, long-lived authenticity, and economic incentives.

Two Halves of the Same 50 Minutes

Migration urgency is a function of resource estimates. Policy rooms keep hearing "migrate now" and "decades away" from different speakers. This breakout holds both halves in one place.

Resource estimates

What would actually be required to break widely used elliptic-curve signatures, under which assumptions, and with which honest error bars. No calendar marketing of a single Q-day.

Migration and agility

Hybrid signatures, staged activation, wallet and L2 impact, post-quantum ZKP where proofs are in the trust path, and MPC where key management takes the hit.

🔗 **Takeaway:** The estimates set the clock. The architecture sets whether the clock can be met without a rushed incident.

What Already Exists — and the Honest Gap

Already standardized

- NIST PQC primitives for KEM and signatures
- Hybrid patterns in adjacent Internet protocols
- National and industry migration handbooks for enterprise stacks

Still missing for DLT

- Agreed migration requirements (correctness, long-term integrity, activation)
- Comparable benchmarks, not screenshots
- A governance path for dormant funds and multi-client stacks

Triage axes that still need a first cut in this room: protection lifetime; impact if broken; migration cost and dependencies. 🔗 **Takeaway:** Do not invent a rival algorithm list. Write the DLT gap on top of NIST schemes.

What BGIN Has Already Started

We are not starting from zero. IKP has been running crypto agility and PQC migration as a standing work item through recent Block meetings.

- Meeting reports from Block 12 through Block 14 on transition, crypto agility, and PQC migration.
- A shared stance: NIST-standardized schemes only; no BGIN algorithm contest; no chain endorsement.
- Japan's government-hosted PQC migration prize, introduced on the next three slides, as one measurement path — not as a second standard.
- Follow-on technical work at BGIN Block #15 (October 2026), including dialogue with NIST.

Takeaway: GDC captures the gaps a 50-minute policy-and-practice room can name. Block 15 is where drafting continues.

Japan's PQC Migration Prize — What It Is

A multi-year, internationally open prize competition on post-quantum migration for public blockchains. Hosted by the Japanese Government (METI/NEDO). BGIN coordinates internationally and runs a neutral evaluation testbed.

It is

- A push to accelerate and de-risk deployment of quantum-resistant signatures and advanced key management.
- Transparent, reproducible evaluation on a geographically distributed academic testbed (BSafe.network).
- A pipeline toward shared practice — not a one-off ceremony.

It is not

- Not a BGIN-owned contest. Japan hosts and funds the prize; BGIN coordinates and evaluates.
- Not a new-algorithm contest. Entries start from NIST-standardized schemes.
- Not chain endorsement, and not a single Q-day calendar claim.

🔗 **Takeaway:** The hard problem on public chains is deployment, evaluation, and migration governance — not selecting a new primitive.

Three Lanes and What Gets Evaluated

Comparative scoring is anchored on Bitcoin and Ethereum. Chain-agnostic work is welcome when it can be mapped to those targets. Themes include PQC migration (formats, hybrid/staged cutover, throughput cost) and advanced key management (MPC, multisig, ZKP). **Takeaway:** Japan funds the prize. BGIN turns shared evidence into standards-ready artifacts. NIST remains the reference for which PQC primitives are in scope.

From This Room to the 2028 Award

Competition / evaluation → BGIN Standard → ISO/TC 307 → Japan's crypto-asset security criteria. Dates are indicative until the host confirms the call. **Takeaway:** This 50 minutes can still change what the call asks teams to prove. Block #15 is the next drafting stop.

What This 50 Minutes Is For

- Document DLT-specific **deployment gaps** — activation, wallets, L2, dormant funds, evidence — rather than re-litigating NIST selections.
- Put **resource estimates** and **migration design** in the same conversation, so urgency is argued from assumptions, not from slogans.
- Name where **post-quantum ZKP** and **MPC** change the key-management and proof path, without turning the hour into a ZKP-only session.
- Align what policymakers, protocol teams, wallet vendors, and evaluation communities each need to see before they can act.

🔗 **Takeaway:** The outcome is a short list of gaps and Block #15 decisions — not a locked migration spec tonight.

Discussion Items for This Room

1. Which objects move first: long-lived confidentiality under harvest-now / decrypt-later, on-chain signatures that must remain verifiable, or the proof and key-management path (PQ ZKP, MPC)?
2. What would make a **resource estimate** usable for a policymaker — assumptions, error bars, and what must not be collapsed into a Q-day date?
3. What must a **neutral testbed** measure so that "PQ-ready" is comparable across stacks?
4. How should **crypto agility** be specified so wallets and ST/PP profiles can rotate algorithms without a fork-by-fork rewrite?

Why a TLS Playbook Will Not Migrate This Stack

A working frame for this breakout

Blockchain Governance Initiative Network

Shin'ichiro Matsuo, Ph.D.

BGIN Co-Chair | Breakout: PQC Migration on DLTs

Global Digital Collaboration | Geneva | 2–3 September 2026

Discussion starter

The writing problem is not a missing algorithm

NIST already standardized the first primitives. Adjacent Internet protocols already have hybrid patterns. The BGIN job is not a rival scheme.

For public ledgers and wallets, migrating in a way that a community can actually run is hard for three stacked reasons:

Public verification

Keys and signatures often sit in the clear. Harvest-now is not only an archival problem.

Consensus freeze

Validity rules are global. You cannot negotiate a cipher suite per connection the way TLS does.

Economic incentives

Dormant funds, wallet UX, miner and custodian costs, and multi-client stacks decide whether a clean design ships.

🔗 **Takeaway:** Design for the next migration now. A rushed cutover creates new incidents; a frozen profile goes stale.

At-Rest versus On-Spend — Timing Is Not One Number

Shor recovers signing keys from exposed public keys. When the public key appears on-chain changes when the attack becomes live.

At-rest

The public key is already on-chain. An adversary can grind offline against a stored verification key until a cryptographically relevant quantum computer can forge spends.

On-spend

The public key is revealed only when funds move. The race is then between the legitimate owner and an attacker who sees the broadcast, not an unbounded offline grind.

Address design, reuse, and wallet defaults therefore change the threat model. A single Q-day slogan erases that difference. **Takeaway:** Resource estimates only become policy-useful when they are tied to which keys are already public.

Questions for this room

This 50-minute breakout is for mapping gaps and naming what Block #15 must decide — not for locking a first migration spec tonight.

1. Which **objects** should BGIN triage first, and which can wait: at-rest keys, on-spend paths, credentials, PQ ZKP, MPC?
2. What would make a **resource estimate** honest enough for this audience — and what language should we refuse (single Q-day, vendor screenshots)?
3. What must a **neutral evaluation** see so that hybrid then cutover is comparable across Bitcoin-class, account-model, and wallet stacks?
4. How should agility be written so ST/PP and wallet profiles can **rotate** without forking the scheme every time the primitive list moves?

Join us at BGIN Block 15

15–16 October 2026 | Georgetown University, Washington, D.C. | In person (remote available). The PQC drafting and measurement work listed above continues in the Block 15 IKP sessions.

Related sessions

- 15 Oct, 09:20–09:50 (Room A). Keynote: PQC
- 15 Oct, 09:50–11:20 (Room B). IKP: PQC Migration
- 15 Oct, 11:30–13:00 (Room B). IKP: PQC Migration (2)

PQC session
bgin-global.org/.../sessions/1-4

Block 15 site
bgin-global.org/events/20261015-block15

Register
eventbrite.com/.../bgin-block15-tickets

Takeaway: Hybrid. Connection details are sent after registration. You are invited.