
BGIN Block#12 Meeting Report

- BGIN is a multi-stakeholder discussion body / distributed think tank.

Transition to Post-Quantum Cryptography / Crypto Agility

**bg
in**

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

© 2023 BGIN (Blockchain Governance Initiative Network) is registered as BN Association, a Japanese general association with its principal place of business at Shiba Building, 704, 4-7-6, Shiba, Minato-ku, Tokyo. All rights reserved.

The know-how described in this document was made available from contributions from various sources, including members of the BGIN and others. Although the BGIN has taken steps to help ensure that the know how is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the know how described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. BGIN and the contributors to this document make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

BGIN Block#12

Transition to Post-Quantum Cryptography / Crypto Agility

Date: Monday, March 3, 2025

Location: Tokyo, Japan

Duration: Approx. 90 minutes

Summary

Explores post-quantum cryptography (PQC) and crypto agility for blockchain. Prepare blockchain for quantum threats to asymmetric cryptography (e.g., digital signatures), risking systems like Bitcoin. PQC transition challenges include long timelines (15+ years), compatibility, and need for blockchain-specific plans beyond NIST's algorithm standards. Discussion about Blockchain-based, long-term timestamping scheme with algorithm renewal to ensure data integrity beyond crypto lifetimes. Debate BGIN's role: Define PQC standards, transition mechanisms, or prioritize crypto agility and threat awareness over immediate migration. BGIN leans toward educating on quantum risks and flexible strategies, avoiding premature PQC mandates.

- Problem Statement on PQC Transition
 - PQC Overview
 - Targets quantum computing risks to asymmetric crypto; symmetric crypto less affected.
 - Quantum break timeline uncertain; past transitions (e.g., 2005) took 15+ years, PQC likely longer.
 - Needs protocols for compatibility, performance, and phased deployment with testing.
 - NIST Efforts
 - Standardizing PQC via competition; selected schemes: CRYSTALS-Dilithium, FALCON, SPHINCS+, FAEST.
 - January 2025 transition document sets deadlines
 - Covers algorithms, not blockchain applications—BGIN could adapt this.
 - Blockchain Risks (2016 Paper)
 - Bitcoin example: Broken SHA-256 enables theft/double-spending; broken ECDSA allows forgery, fake alerts.
 - Impacts layer 2 (e.g., zero-knowledge proofs) if crypto fails.
 - Crypto Agility
 - Ability to switch primitives if compromised; aims for rapid updates without infrastructure overhaul.
 - 2017 idea: Wrap old signatures with secure, long-term schemes (LTB).
- Blockchain-Based Long-Term Timestamping
 - Concept
 - Proposes timestamping to prove data existence over time.
 - Traditional timestamping via TSAs vulnerable to malice or crypto breaks.
 - Blockchain Benefits
 - Decentralized, tamper-resistant, verifiable.

- Security tied to client-side hash and blockchain crypto (hash/signatures).
- Long-Term Issue
 - Quantum or lifecycle threats could invalidate timestamps for decades-long data (e.g., government, art).
 - Solution: Renew weak algorithms (e.g., SHA-1 to SHA-2, RSA to FALCON) before full compromise.
- Scheme Details
 - Formal model prevents tampering, backdating, forging via renewals.
 - Blockchain-side: Group blocks, rehash with stronger functions; transfer assets to new keys.
- Client-side options: Upload raw data (no privacy), renew hash chain, or link tokens (latest only needed).
- Discussion: Potential BGIN Work Items
 - Proposals
 - Define PQC blockchain requirements (no current standard); create transition plans for non-PQC chains.
 - Scope: Focus on signatures, consider encryption for secrecy (e.g., long-term data).
 - Perspectives
 - Quantum “treasure hunters” could claim unupdated Bitcoin; incentive exists, but logistics tricky.
 - Market may self-correct (e.g., key update services), but quantum risk downplayed (20-30 years off).
 - Client updates are costly; agility over rigid PQC mandates avoids fragmentation.
 - Migration Dynamics
 - Browsers update cheaply; Bitcoin’s decentralized nature makes it harder, costlier.
 - Past migrations (e.g., SHA-1) took 20+ years; Bitcoin’s 20-year signatures heightened urgency.
 - Strategic Options
 - Warning first: Highlight crash risk (e.g., Bitcoin chaos post-quantum break).
 - Agility focus: Flexible designs buy time vs. immediate PQC push.
 - Governance: Hybrid signatures, custody could simplify transitions.
- Next steps:
 - Raise quantum threat awareness, explore agility, delay specific PQC solutions.