# BGIN REPORT: CRYPTO AGILITY AND PQC MIGRATION

Post-Session Comprehensive Summary

## I. Executive Summary

This session focused on the existential challenges and strategic pathways for migrating blockchain technologies, specifically Bitcoin and Ethereum, to post-quantum cryptography (PQC). While some estimates place the arrival of cryptographically relevant quantum computers (CRQCs) within 3 to 4 years, the session emphasized that Crypto Agility must be addressed as a general protocol requirement. The discussion moved beyond theoretical threats to analyze real-world hurdles: the “Burn vs. Steal” dilemma for dormant assets, the lack of standardized evaluation criteria for “Quantum Secure” protocols, and the complexity of updating decentralized infrastructures. Key outcomes included a proposal for a multi-year BGIN research project to analyze stakeholder incentives and the potential for LLM-driven formal verification to secure new PQC standards.

## II. Key Discussion Points

- Technological and Ideological Challenges
    - Negotiation vs. Consensus: Unlike point-to-point protocols (e.g., TLS) that use cipher suites to dynamically negotiate algorithms, blockchains cannot easily negotiate among an unbounded number of nodes without risking forks.
    - Transition Vulnerabilities: Asynchronous updates across nodes during migration periods increase fragility to 51% attacks.
    - The Immutability Paradox: Bitcoin’s greatest innovation—immutability—is now its “Achilles heel,” as legacy addresses (Pay-to-Public-Key) are vulnerable to quantum discovery.
- Incentive Models and User Adoption
    - Short-termism: Many stakeholders (miners/nodes) prioritize short-term price stability over long-term security. Discussions of migration can be perceived as a threat to asset value, leading to “cognitive dissonance” in the community.
    - The “Burn vs. Steal” Dilemma:
        - Burn: Forcing active migration disenfranchises owners of dormant/lost accounts (e.g., Satoshi-era coins).

        - Steal: Making migration optional allows quantum attackers to steal legacy funds, resulting in a non-consensual wealth redistribution to whoever builds the first CRQC.
- Complexity of Ecosystem & Modular DSAs
    - The ecosystem (wallets, nodes, oracles, miners, hardware) must be updated simultaneously.
    - Modular DSAs: A proposal was made for a modular architecture where Digital Signature Algorithms (DSAs) are pluggable, allowing governance to swap compromised algorithms for stronger backups without rebuilding the chain.
- Historical Precedents & “Benevolent Dictators”
    - Ethereum’s Merge: The transition from PoW to PoS took several years even under a “benevolent dictator,” illustrating that decentralized migration is inherently slow.
    - 2018 Incident: A 2018 Bitcoin inflation vulnerability was managed by developers privately reaching out to miners—a “direct negotiation” model that contrasts with the ideal of decentralized transparency.
- Research and Indicators
    - The Manhattan Project Parallel: Quantum breakthroughs are likely being developed in state-funded secrecy.
    - Proxies for Urgency: Quantum attacks on non-blockchain systems could serve as “clouds turning gray” indicators for the industry to hasten migration.

# III. Detailed Session Summary

1. Lightning Talk: The Framework of Crypto Agility

The talk distinguished between specific PQC Migration and general Crypto Agility.

- Three Pillars of Difficulty:
    1. Consensus Constraints: Unlike TLS, blockchains cannot dynamically negotiate “cipher suites” without risking massive forks.
    2. The Fragile Window: Asynchronous node updates create a window where the network is vulnerable to 51% attacks.
    3. Economic Resistance: Stakeholders often prioritize short-term price stability over long-term security.
- Requirements: Proposed that any PQC transition must ensure signature unforgeability, early adoption incentives, and address preservation to maintain market consistency.

2. Quantum Resistant Ledger (QRL): Practical PQC

QRL was presented as a 7-year “geriatric” proof-of-concept that has used NIST-standard XMSS since block one.

- Zond (QRL 2.0): Introduced the Zond hard fork, which adds EVM compatibility and moves to PoS, providing a “Quantum Insurance Policy” for Ethereum developers to recompile Solidity code in a secure environment.

- Manhattan Project Analogy: The presenter argued that “Q-day” will not be publicized; nation-states will keep breakthroughs secret to exploit financial and national security targets.

3. Formal Verification & LLM Agents

Presented a pipeline to ensure the mathematical soundness of PQC standards like TSL (Top Single Layer) encoding.

- Verification vs. Hallucinations: Detailed a 4-stage process: Informal Proof → Peer Review → Formalization (Lean) → Machine Verification. This ensures the final proof is mathematically absolute and independent of the LLM used to generate it.

4. Open Discussion: The Road to BGIN Block 14

- The “Burn vs. Steal” Dilemma: A collaborative debate on the ideological conflict for Bitcoin (BIP 360).
    - Burn: Protecting the network by forcing active migration, effectively “burning” dormant Satoshi-era coins.
    - Steal: Maintaining user property rights by leaving funds accessible, effectively allowing quantum-capable entities to “steal” legacy wealth.
- The Criteria Gap: Participants emphasized that we are “flying blind.” We lack a methodology to audit an entire blockchain protocol for quantum fragility beyond its signature scheme.
- Hash and Parameter Migration: Noted that agility must include hash functions; output sizes may need to double to defend against Grover’s Algorithm, adding further complexity to state-bloat issues.

IV. Action Items and Next Steps

1. Establish Evaluation Criteria for Quantum Secure Protocols
    - Develop a methodology to verify if a combined blockchain protocol (not just cryptographic primitives) is quantum-resistant
    - Address the gap that NIST evaluates primitives, but no standardized criteria exist for protocol-level quantum security assessment

2. Define PQC Migration Requirements
    - Formalize core requirements: signature unforgeability, dormant account support, early adoption incentives, and address preservation
    - Include hash function migration requirements (output size considerations for Grover resistance)
    - Establish clear timelines for disabling legacy DSAs (ECDSA, BLS) post-migration—a topic currently absent from most proposals

3. Initiate BGIN Research Project
    - Goal: Publish a study/research report within 2-3 years covering the entire blockchain ecosystem

- Focus: Analyzing stakeholder incentives and defining “Quantum Secure Protocol” requirements to cover all complex ecosystems

4. Community Outreach
Collaborate with different blockchain communities to gather diverse perspectives on PQC migration.

- Organize follow-up sessions or workshops to further discuss and refine the research project.
- Circulate anonymized meeting report to all participants immediately

# V. Conclusion

The session concluded with a stark realization: the “Chicken Race” against quantum development is underway. Whether through a “Tidal Wave” (sudden Black Swan) or a “Tide” (gradual migration), the industry must move toward modularity and formal verification. The proposal to create a new BGIN research project was met with consensus as the essential next step.