Dilithion

A Post-Quantum Cryptocurrency

Technical Whitepaper Version 1.0

October 2025

Launch Date: January 1, 2026, 00:00:00 UTC

Abstract

Dilithion is a decentralized cryptocurrency designed from the ground up for the post-quantum era. As quantum computers advance toward breaking classical cryptographic systems like ECDSA and RSA, the need for quantum-resistant blockchain technology becomes critical. Dilithion addresses this threat by implementing CRYSTALS-Dilithium, a NIST-standardized post-quantum digital signature scheme, combined with RandomX proof-of-work for ASIC-resistant CPU mining.

This whitepaper presents Dilithion's technical architecture, consensus parameters optimized for large post-quantum signatures, economic model, and roadmap for sustainable decentralized currency in the quantum age.

> **Key Features:**
>
> - **Post-quantum security:** CRYSTALS-Dilithium (NIST FIPS 204)
> - **ASIC-resistant mining:** RandomX proof-of-work
> - **Optimized consensus:** 4-minute blocks for large signature propagation
> - **Fair distribution:** No premine, pure proof-of-work launch
> - **Fixed supply:** 21 million coins
> - **Launch:** January 1, 2026, 00:00:00 UTC

Table of Contents

1. Introduction: The Quantum Threat

1.1 The Problem

Modern cryptocurrency security relies on classical cryptography:

- **ECDSA (Bitcoin, Ethereum):** Elliptic Curve Digital Signature Algorithm
- **RSA:** Rivest-Shamir-Adleman encryption
- **SHA-256:** Secure Hash Algorithm (for mining)

Shor's Algorithm (1994) demonstrated that quantum computers can break ECDSA and RSA in polynomial time. While SHA-256 mining receives only a modest speedup (Grover's algorithm), **digital signatures are critically vulnerable**.

1.2 Timeline to Quantum Threat

Current State (2025):

- IBM: 1,121-qubit quantum computer (Condor)
- Google: Quantum supremacy claimed
- China: Pan-Jianwei's quantum network

Expert Estimates:

- **2030-2035:** Cryptographically relevant quantum computers (CRQC)
- **Breaking Bitcoin:** Estimated 1,500-3,000 logical qubits required
- **Current trajectory:** Doubling qubits every ~2 years

Conclusion: Cryptocurrencies must transition to post-quantum cryptography **now** to remain secure over their multi-decade lifespan.

1.3 Existing Cryptocurrency Vulnerability

Cryptocurrency	Signature Scheme	Quantum Vulnerable?	Migration Plan?
Bitcoin	ECDSA	✅ Yes	None announced
Ethereum	ECDSA	✅ Yes	Research phase only
Litecoin	ECDSA	✅ Yes	None announced
Monero	EdDSA	✅ Yes	None announced
Dilithion	**Dilithium3**	**❌ No**	**Built-in from genesis**

Critical Issue: Retrofitting existing blockchains with post-quantum cryptography requires:

- Hard fork (community consensus required)

- Wallet migrations (user action required)
- Backward compatibility challenges
- Risk of botched transition

Dilithion's Solution: Start with post-quantum cryptography from genesis block.

2. Post-Quantum Cryptography

2.1 CRYSTALS-Dilithium

Selection Process:

- NIST Post-Quantum Cryptography Standardization (2016-2024)
- 82 initial submissions
- Multiple rounds of evaluation
- **Winner:** CRYSTALS-Dilithium (2022)
- **Standardized:** FIPS 204 (August 2024)

Why Dilithium?

1. **Security:** Based on hard lattice problems (Module-LWE, Module-SIS)
2. **Performance:** Fast signing and verification
3. **Standardization:** Official NIST standard
4. **Analysis:** Years of public cryptanalysis, no serious breaks
5. **Versatility:** Three security levels (Dilithium2, 3, 5)

Dilithion uses Dilithium3:

- **Security level:** NIST Level 3 (equivalent to AES-192)
- **Public key size:** 1,952 bytes
- **Signature size:** 3,309 bytes
- **Signing speed:** ~1-2 milliseconds
- **Verification speed:** ~1 millisecond

2.2 Comparison to Classical Cryptography

Metric	ECDSA (secp256k1)	Dilithium3	Ratio
Public key	33 bytes	1,952 bytes	59x larger
Signature	72 bytes	3,309 bytes	46x larger
Security	~128-bit	192-bit (quantum-safe)	More secure
Signing time	<1 ms	1-2 ms	Comparable
Verify time	~1 ms	~1 ms	Identical
Quantum safe?	❌ No	✅ Yes	Critical advantage

Trade-off: Dilithion transactions are ~15x larger than Bitcoin transactions, but provide quantum resistance.

Continue reading for complete technical specifications, economic model, security analysis, and launch roadmap...

For the complete whitepaper, please refer to WHITEPAPER.md
This HTML preview shows the structure and formatting.
The full document contains 1,100+ lines covering all technical and economic details.

8. Conclusion

8.1 Why Dilithion Matters

The Quantum Threat is Real:

- Timeline: 5-10 years to cryptographically relevant quantum computers
- Existing cryptocurrencies are vulnerable
- Transition will be difficult and contentious
- **Action needed now**

Dilithion's Solution:

- Built quantum-safe from genesis
- No migration required
- Users protected from day one
- Proven cryptography (NIST standard)

8.2 Technical Excellence

Optimized for Post-Quantum Era:

- 4-minute blocks accommodate large signatures
- Balanced emission schedule (31.3% Year 1)
- Affordable transaction fees
- ASIC-resistant CPU mining
- Professional-grade security

8.3 Fair Launch Principles

Dilithion adheres to fair launch principles:

- ✅ No premine
- ✅ No ICO / token sale
- ✅ No founder allocation

- ✅ No venture capital pre-allocation
- ✅ Pure proof-of-work from genesis
- ✅ Open-source (MIT license)
- ✅ Community-driven development

Everyone starts equal on January 1, 2026.

8.4 Long-term Vision

Dilithion aims to be:

1. **The standard** for quantum-safe cryptocurrency
2. **A store of value** in the post-quantum era
3. **A medium of exchange** with reasonable fees
4. **A platform** for decentralized applications
5. **A community** of quantum-aware developers and users

> ***Mission Statement:*** *"Secure digital currency for the quantum age, built by the community, for the community."*

Technical Specifications Summary

Parameter	Value
Launch Date	January 1, 2026, 00:00:00 UTC
Total Supply	21,000,000 DIL
Block Time	4 minutes (240 seconds)
Block Reward	50 DIL (halves every 210,000 blocks)
Halving Interval	Every 210,000 blocks (~1.6 years)
Signature Algorithm	CRYSTALS-Dilithium3 (NIST FIPS 204)
Hash Algorithm	SHA-3-256 (NIST FIPS 202)
Mining Algorithm	RandomX (Monero-derived, ASIC-resistant)
Difficulty Adjustment	Every 2,016 blocks (~5.6 days)
Transaction Fee	0.0005 DIL base + 25 sats/byte

Dilithion Whitepaper v1.0

October 2025

"Quantum-Safe. Community-Driven. Fair Launch."

Disclaimer: This whitepaper is for informational purposes only and does not constitute investment advice. Cryptocurrency investments carry risk. DYOR (Do Your Own Research). Dilithion is experimental software released as open-source. No guarantees are made regarding future value, adoption, or success.