



FRIOTAÍOCH · FRIO

— TECHNICAL BRIEF · V1.0

A post-quantum proof-of-work cryptocurrency.

Bitcoin-derived consensus, hardened with NIST-standardised quantum-resistant signatures. Coins secured by ML-DSA and SPHINCS+, spendable from the browser.

Overview

Friotaíoch (FRIO) is a proof-of-work cryptocurrency derived from Bitcoin Core that adds native support for post-quantum digital signatures. It introduces Pay-to-Quantum-Resistant (P2QR) outputs backed by two NIST-standardised signature schemes, allowing coins to be received and spent using cryptography believed to resist attack by large-scale quantum computers, while retaining Bitcoin's SHA-256d proof-of-work and UTXO model.

The network launched cleanly from its own genesis block with no premine and no pre-allocation. Consensus, block structure, and transaction validation follow Bitcoin Core except where deliberately changed for post-quantum support and network identity. A browser-based, non-custodial wallet performs quantum-resistant signing entirely client-side in WebAssembly.

02 — MOTIVATION

The quantum exposure of UTXO chains

Bitcoin and its derivatives authorise spending with ECDSA and Schnorr signatures over the secp256k1 curve. The security of these schemes rests on the hardness of the elliptic-curve discrete logarithm problem — a problem that a sufficiently large, fault-tolerant quantum computer running Shor's algorithm could solve efficiently.

The practical exposure is concentrated at the moment of spending. When a transaction is broadcast, it reveals the public key authorising the output. An adversary able to derive the private key from that public key — before the transaction confirms, or against any address whose public key is already known — could forge a competing spend. Reused addresses, and any output whose script exposes a raw public key, widen this surface further.

Post-quantum signature schemes remove this dependency on elliptic-curve hardness. Friotaíoch's design question is narrow and concrete: **what does a Bitcoin-style chain look like if the signatures that authorise spending are quantum-resistant from the first block?**

SCOPE

Friotaíoch is an experimental, independently built system. Its cryptographic components are drawn from standardised primitives but the integration as a whole is unaudited. It is presented as a working experiment, not as production financial infrastructure.

Pay-to-Quantum-Resistant outputs

Friotaíoch adds a new class of output script, P2QR, committing coins to a post-quantum public key. Two schemes are supported, each occupying a distinct SegWit witness version so they are unambiguously distinguished at the consensus layer.

SCHEME	STANDARD	WITNESS	PROFILE
ML-DSA-65	FIPS 204	v2	Lattice-based (Dilithium). Compact signatures, fast verification.
SPHINCS+-SHA2-128s	FIPS 205	v3	Hash-based (SLH-DSA). Conservative security, larger signatures.

Offering both a lattice-based and a hash-based scheme is deliberate. ML-DSA provides efficient, compact signatures suited to everyday use; SPHINCS+ rests on minimal assumptions — the security of its underlying hash function alone — and acts as a conservative hedge should weaknesses emerge in lattice assumptions. Users choose their trust model per address.

Consensus enforcement

P2QR validation is enforced by a dedicated script-verification flag (`SCRIPT_VERIFY_PQR`) active from genesis, so no signalling window or activation height exists in which quantum-resistant outputs are unenforced. Both schemes are validated at build time against pinned NIST known-answer test vectors to guarantee conformance to the standards.

Denial-of-service protection

Post-quantum signatures are larger and more expensive to verify than ECDSA. To prevent verification cost from becoming an attack vector, each block carries a bounded post-quantum verification budget, capping the aggregate PQC verification work a single block can impose on the network.

KEY HANDLING

Post-quantum private keys are generated, stored, and encrypted at rest by the wallet. Signing occurs locally; keys are never transmitted. The reference node exposes P2QR address generation, receipt, persistence, signing, and spending through its RPC interface.

Address types

Friotaíoch supports the full range of Bitcoin-style address types alongside the two post-quantum P2QR types, so users can transact with classic or quantum-resistant outputs as they choose.

Legacy (P2PKH)	F...	Base58Check
P2SH	7...	Base58Check
SegWit v0	friolq...	bech32, P2WPKH
Taproot	friolp...	bech32m, witness v1
P2QR · ML-DSA-65	friolz...	bech32m, witness v2 · post-quantum
P2QR · SPHINCS+-128s	friolr...	bech32m, witness v3 · post-quantum

All witness-based types share the human-readable prefix `frio` . The two post-quantum types are encoded as higher witness versions, making them forward-compatible with existing address tooling while remaining distinguishable to the consensus layer.

Chain parameters

PROPERTY	VALUE
Ticker	FRI0
Proof of work	SHA-256d
Difficulty adjustment	ASERT (aserti3-2d), per-block
Target block time	10 minutes
Block reward	50 FRI0, halving every 210,000 blocks
Supply cap	21,000,000 FRI0
Premine	None
Network magic	F710C0DE
P2P / RPC port	51775 / 51777
Genesis hash	00000000908e647ce8296582a2d24023ef96a5e7d2320a5815b603463993676d

Friotaíoch uses ASERT (Absolutely Scheduled Exponentially Rising Targets), anchored at the

Browser-native quantum signing

Friotaíoch provides a non-custodial web wallet that performs post-quantum signing entirely in the browser. The ML-DSA and SPHINCS+ implementations are compiled to WebAssembly and executed client-side; private keys are generated and held locally and never leave the device.

The wallet supports both classic and quantum (P2QR) send and receive. It derives P2QR receive addresses, selects and signs across multiple inputs, and constructs change outputs — all locally — before broadcasting the finished transaction. This keeps the trust model self-custodial while making the post-quantum address types usable without running a full node.

Peer-to-peer and infrastructure

The network is a standard Bitcoin-family peer-to-peer gossip network. Nodes discover peers through a DNS seeder and may connect over clearnet or Tor; the reference deployment operates both a reachable clearnet node and a Tor hidden-service node, bridging the two. A block explorer, an ElectrumX server, and a live node map are operated as public infrastructure.

SERVICE	ENDPOINT
Website	friotaioch.com
Block explorer	explorer.friotaioch.com
Browser wallet	wallet.friotaioch.com
DNS seed	seed.friotaioch.com

Status and intent

Friotaíoch is live on mainnet, mining under ASERT, with the full post-quantum wallet stack operational. It is released under the MIT license as a derivative work of Bitcoin Core, built and maintained openly by an independent developer.

It is offered in the spirit of an experiment: a concrete, running answer to the question of what post-quantum security looks like on a Bitcoin-derived chain. It has not undergone formal security audit, and readers should treat it accordingly.

NO INVESTMENT CLAIM

This document is a technical description. It is not financial advice and makes no representation as to the value, price, or investment merit of FRIO.