QCoin: A Progress-Free Proof-of-Work Protocol for a Post-Quantum World

Version 1.2 - Public Specification

Author: QCoin Research Group

Date: October 23, 2025

Abstract

We propose **QCoin**, a peer-to-peer electronic cash system designed for long-term security in a post-quantum world. The protocol is built upon the foundational principles of Bitcoin but introduces several critical innovations: a post-quantum signature scheme (CRYSTALS-Dilithium) mandated from genesis, a modern hash algorithm (BLAKE3), and a novel, grind-resistant Proof of Work (PoW) mechanism. This paper specifies a consensus algorithm based on a memory-hard, **progress-free, i.i.d. (independent and identically distributed) trial structure**. The work scoring and difficulty retargeting are probabilistically grounded to ensure network stability and resist selfish mining. The initial distribution of the native currency will be derived from a preliminary token on the Polygon network, allowing early supporters to become the foundational stakeholders of the mainnet.

---

1. Introduction

The success of Bitcoin has demonstrated that a decentralized, trustless network can maintain a secure and immutable ledger. The core of this innovation is Proof of Work, which solves the double-spending problem by making it computationally impractical for an attacker to rewrite the transaction history. QCoin is proposed as a successor protocol that retains Bitcoin's core economic model while addressing its known and future vulnerabilities. The primary design goals are: 1) Immediate security against quantum adversaries. 2) A fair, decentralized, and ASIC-resistant mining process. 3) A stable and predictable monetary policy.

2. Core Components

QCoin mandates **CRYSTALS-Dilithium2** for all transaction signatures, forgoing ECDSA entirely. This ensures that ownership of funds is secure against attacks from future fault-tolerant quantum computers using Shor's algorithm. The address format will be adapted from standard Bitcoin formats (e.g., Bech32m) to accommodate the larger public key size.

All internal cryptographic hashing (for Merkle trees, block headers, etc.) will use **BLAKE3** for its superior performance and security properties compared to SHA-256.

3. Proof of Work: A Memory-Hard, Grind-Resistant Puzzle

To achieve fairness and decentralization, the PoW puzzle must be **progress-free** (each attempt is independent) and **grind-resistant** (miners cannot pre-scan for "easy" puzzles). Optimization-based puzzles that allow for continuous improvement on a single instance are inherently not progress-free and are thus rejected.

1. **Seed Generation:** The seed for each trial is `S = BLAKE3(prev_hash || merkle_root || nonce || miner_counter)`. The `nonce` is a 128-bit field in the header, and `miner_counter` is an additional unbounded field controlled by the miner.
2. **Memory-Hard Graph Construction:** The seed `S` is used to deterministically generate a large, pseudo-random directed acyclic graph (DAG), requiring significant RAM (e.g., >1 GB) to hold in memory.
3. **Single-Shot Evaluation:** The "work" is to find a specific property within this generated graph (e.g., finding a path that results in a specific hash, or solving a constrained pointer-chasing problem). This is a **one-shot evaluation**; a given graph either contains the solution property or it does not.

This design ensures each trial is an independent event, restoring the lottery-like property of traditional PoW and creating a strong barrier to ASIC development.

4. Difficulty, Work, and Fork Choice

A block is valid if the hash of its solution proof is less than a target value derived from the current network difficulty, `D`.

The difficulty `D` is adjusted every 2,016 blocks using a Bitcoin-like formula with clamping `[0.25, 4.0]` to maintain an average block time of 600 seconds.

The valid chain is the one with the highest **cumulative difficulty** (sum of `D` for all blocks). In the event of a tie, the chain whose most recent block has the lower header hash is chosen.

5. Network Protocol and Economics

Nodes will not accept a block header as a valid tip for mining unless the full block body is present and fully validated, preventing certain DoS vectors.

A "block weight" concept similar to SegWit will be used to account for the large size of Dilithium2 signatures (~2.4 KB), creating a predictable fee market.

6. Tokenomics and Issuance

The protocol enforces a hard cap of 21 million native QCoin (QCN). The block reward starts at 50 QCN and follows Bitcoin's halving schedule, reducing by 50% every 210,000 blocks.

The QCoin mainnet will launch with a genesis block containing no developer premine or treasury. The **initial distribution of the native currency (QCN) will be allocated to the holders of the preliminary QCoin token on the Polygon network.**

A snapshot of Polygon token holders will be taken at a pre-announced block height prior to the mainnet launch. These holders will be able to claim their native QCN via a one-way burn or bridge mechanism, ensuring that the project's earliest supporters become the foundational stakeholders of the new network. This process serves as the sole method for the initial creation and distribution of QCoin.

7. Conclusion

This paper has presented a formal specification for QCoin. By learning from the theoretical and practical limitations of previous protocols, we have designed a system with a strong foundation for long-term security and decentralization. The use of a progress-free, memory-hard PoW, combined with post-quantum cryptography from genesis and a robust economic model, makes QCoin a credible and forward-looking proposal for the future of peer-to-peer digital currency.

8. Project Information & Implementation

The QCoin project is an open, community-driven research initiative. Development is funded by the preliminary QCoin token on the Polygon network, which also functions as the distribution vehicle for the mainnet launch. A reference implementation of this protocol will be developed and released under an MIT license for peer review. A public testnet will be launched to validate the protocol's stability, security, and economic assumptions. For the latest updates, technical discussions, and information on the reference implementation, please consult the official project resources.

- **Official Website:** https://proofofquantum.org
- **Community Research Group:** Join the discussion on Telegram @QCoinResearchGroup

---

Appendix A: Protocol Parameters

Parameter	Symbol	Default Value	Notes
Target Block Time	`T`	600 seconds	10 minutes
Difficulty Retarget Interval	`N_retarget`	2,016 blocks	Approx. 2 weeks
Block Reward Halving Interval	`N_halving`	210,000 blocks	Approx. 4 years
Block Weight Limit	`W_max`	4,000,000 WU	Similar to SegWit
PoW Nonce Size	-	128 bits	In block header
Digital Signature Algorithm	-	CRYSTALS-Dilithium2	NIST Post-Quantum Standard
Internal Hash Algorithm	`H()`	BLAKE3	
Ticker Symbol (Mainnet)	-	QCN	