ChatGPT

QKey White Paper

Abstract

QKey is a post-quantum ownership registry and recovery protocol. It links existing blockchain addresses (Bitcoin, Ethereum, and other EVM chains) to quantum-secure Dilithium public keys through on-chain commitments that users can self–verify. Every commitment and recovery action is executed by simple smart-contract calls; no external validator set, Merkle tree, or off-chain consensus is required. The QKEY utility token powers registration, staking, and quadratic-weighted (polynomial) DAO governance while funding grants that advance quantum-resilient security.

1 Tokenomics

1.1 Supply Parameters

- **Max supply:** 1 000 000 000 QKEY (fixed, non-inflationary)
- **Decimals:** 18
- **Initial circulating supply at TGE:** 8 % (community and launch liquidity)

1.2 Allocation

Bucket	% of Max	Vesting	Rationale
Foundation reserve	20 %	12-month cliff, 48-month linear	Long-term protocol development
Core team	15 %	6-month cliff, 36-month linear	Talent retention
Staking reward emissions	15 %	Distributed per-block over 10 years	Incentivise QKEY staking for spam-resistance and network health
Community incentives & airdrops	10 %	0–12 month linear	Grass-roots adoption
Ecosystem grants	10 %	Released on DAO approval	Integrations & R&D
Coin-recovery grant pool	10 %	Locked, unlocked by polynomial DAO vote	Funds lost-key recovery grants
Public sale (OpenPrice Offering on Base)	5 %	No lock	Price discovery & liquidity

Bucket	% of Max	Vesting	Rationale
Consulting & partnership pool	5 %	Vests with partner milestones	Enterprise pilots
Treasury liquidity management	10 %	Unlocked; governed	Market support

1.3 Vesting Mechanics

Time-locked escrow contracts enforce linear vesting. Any unclaimed staking emissions after 10 years are burned. Grant-pool tokens are non-transferable until a DAO vote approves a specific grant.

1.4 Multi-Chain Plan

- **Phase 0:** Base main-net (low fees, deep L2 liquidity)
- **Phase 1:** Canonical bridge to Ethereum main-net for institutional custody
- **Phase 2:** Permissionless bridging to BNB Chain, Arbitrum, Optimism
- **Phase 3:** Non-EVM bindings—Bitcoin OP_RETURN anchors and a Cardano side-car

2 Purpose and System Overview

2.1 Problem Statement

Classical signatures such as ECDSA/Schnorr will become vulnerable once scalable quantum computers are available. Holders need a forward-compatible way to attach quantum-safe credentials before “harvest-now-decrypt-later” attacks succeed.

2.2 Solution Overview

The QKey protocol lets any wallet generate a NIST-standard Dilithium keypair and publish a salted hash commitment (URI prefix `pqd:`) to their existing address. After a safety delay, the user (or anybody) reveals the pre-image along with a Dilithium signature proving key ownership. The smart contract verifies the signature and permanently binds the quantum key to the classical address.

2.3 Commit-and-Reveal Workflow (no new consensus engine)

1. **Commit (tx_1):** `commitDilithiumKey(bytes32 hash, uint256 fee)` stores the opaque hash and burns 10 QKEY.
2. **Reveal (tx_2):** `revealDilithiumKey(pubKey, salt, address, sig)` checks that `hash==H(pubKey‖salt‖address)` and that `sig` is a valid Dilithium signature over `address`. Success finalises the binding.

This two-step process is entirely voluntary—the base chain’s existing consensus secures ordering. No extra validator set, Merkle root, or off-chain checkpoints are necessary.

3 Revenue Model and Token Utility

1. **Key-signing fees** – Each commitment burns 10 QKEY; 30 % equivalent is re-minted to the staking-rewards pool, 20 % flows to the DAO treasury.
2. **SDK licensing** – Wallets and custodians pay recurring licences (fiat or QKEY). Half of receipts buy and burn QKEY; half fund ecosystem grants.
3. **Coin-recovery grants** – Users seeking help with lost keys post a QKEY stake; approved cases receive a grant from the grant pool to subsidise tooling and audits.
4. **Consulting** – Enterprise migration projects are billed in QKEY or USDC and routed through the treasury.
5. **Membership utility** – Holding $\geq$10 000 QKEY unlocks rate-limited API calls; holding $\geq$1 % of circulating supply grants proposal rights in the DAO.
6. **Staking rewards** – Stakers lock QKEY to receive a share of per-block emissions and a pro rata portion of the re-minted commitment fees.
7. **Polynomial DAO voting** – Voting weight scales with the square-root of tokens staked (quadratic voting), mitigating whale dominance. Treasury disbursements, grant approvals, and parameter changes all pass through this mechanism.

4 Protocol Architecture

Layer	Component	Description
Smart contracts	`QKeyRegistry`	Stores commitments, verifies reveal signatures, manages fee burning and re-mint
Smart contracts	`StakingPool`	Handles lock-up, reward distribution, and quadratic vote weight snapshots
SDK / Wallet plugin	Keygen + commit UI	Generates Dilithium keys, builds commit & reveal txs
Optional off-chain	Watch service	Monitors chain for un-revealed commits and nudges users to reveal
Governance	DAO contracts	Polynomial voting, grant scheduling, parameter updates

Recovery flow – A claimant submits evidence plus a refundable QKEY stake. If a DAO vote approves, a one-time recovery smart-contract pathway enables the asset transfer; grant-pool tokens cover external audit or legal costs.

Security parameters: Dilithium III, 32-byte salted hash, optional periodic Bitcoin timestamping for additional integrity (out-of-scope of core protocol).

5 Quantum-Technology Landscape

Milestone	Year	Impact
NIST selects Dilithium & Falcon	2022	Establishes PQ signature baseline

Milestone	Year	Impact
IBM "Heron" 133-qubit logical demo	2024	First error-corrected qubit
Google "Aquila" 1 000-qubit roadmap	2025	Commercial fault-tolerant target 2029
Large-scale photonic cluster (>10 000 qubits)	2025	Alternative path beyond transmons
US government harvest-now-decrypt-later memo	2024	Accelerates migration timelines

Experts estimate ~20 M physical qubits and 8–12 hours runtime to break 256-bit ECDSA. Conservative forecasts place “Q-day” within the next decade. QKey offers forward secrecy now, without disruptive chain forks.

6 Corporate, Trademark & Legal

QKey Foundation, a Delaware Public Benefit Corporation, stewards the open-source code (MIT licence). “QKEY” and the key-in-Q glyph are filed trademarks (USPTO #98/XXXXXX). This document describes technology and does **not** constitute an offer to sell, or solicitation to buy, any security. QKEY tokens provide consumptive utility—payment for protocol functions, staking, and DAO participation. No profit expectation is marketed.

Risk factors include regulatory changes, smart-contract exploits, cryptographic advances, and digital-asset volatility. Consult qualified advisers before participating.