QRDX Protocol Whitepaper v2.0

QRDX Foundation Research Team

November 3, 2025

Contents

1 QRDX Protocol Whitepaper v2.0 **1**
1.1 Quantum-Resistant Decentralized Exchange & Asset Shielding Protocol 1
1.2 Abstract 2
1.3 Table of Contents 2
1.4 1. Introduction 2
1.5 2. The Quantum Threat 3
1.6 3. QRDX Chain Architecture 4
1.7 4. Post-Quantum Cryptography Implementation 5
1.8 5. QRDX Protocol: Quantum-Resistant AMM 6
1.9 6. Asset Shielding Mechanism 7
1.10 7. qRC20 Token Standard 8
1.11 8. Cross-Chain Bridge Infrastructure 9
1.12 9. Consensus Mechanism 11
1.13 10. Tokenomics 12
1.14 11. Governance Model 13
1.15 12. Security Analysis 14
1.16 13. Performance Benchmarks 16
1.17 14. Roadmap 17
1.18 15. Conclusion 18
1.19 16. References 18
1.20 Appendix A: Glossary 19
1.21 Appendix B: Mathematical Formulas 20
1.22 Appendix C: Contract Addresses (Mainnet - Post Launch) 21

1 QRDX Protocol Whitepaper v2.0

1.1 Quantum-Resistant Decentralized Exchange & Asset Shielding Protocol

Version: 2.0
Last Updated: November 3, 2025
Authors: QRDX Foundation Research Team
Contact: research@mail.qrdx.org

1.2 Abstract

The emergence of quantum computing threatens the cryptographic foundations of blockchain technology. QRDX addresses this existential challenge by introducing the first quantum-resistant decentralized exchange protocol with native asset shielding capabilities. Built on Uniswap v3 and v4 architecture principles and secured by NIST-standardized post-quantum cryptographic algorithms, QRDX enables users to shield traditional assets (e.g., ETH → qETH) into quantum-resistant equivalents while maintaining the efficiency and capital utilization of modern automated market makers (AMMs).

QRDX Chain serves as the foundational Layer-1 blockchain implementing post-quantum security primitives, enabling cross-chain asset migration, decentralized trading, and long-term cryptographic security. This whitepaper presents the technical architecture, economic model, and security guarantees of the QRDX ecosystem.

1.3 Table of Contents

1. Introduction
2. The Quantum Threat
3. QRDX Chain Architecture
4. Post-Quantum Cryptography Implementation
5. QRDX Protocol: Quantum-Resistant AMM
6. Asset Shielding Mechanism
7. qRC20 Token Standard
8. Cross-Chain Bridge Infrastructure
9. Consensus Mechanism
10. Tokenomics
11. Governance Model
12. Security Analysis
13. Performance Benchmarks
14. Roadmap
15. Conclusion
16. References

1.4 1. Introduction

1.4.1 1.1 Background

Blockchain technology relies on cryptographic primitives that are vulnerable to quantum computing attacks. Shor's algorithm, running on a sufficiently powerful quantum computer, can break elliptic curve cryptography (ECC) and RSA encryption—the backbone of current blockchain security. With major technology companies and governments investing billions in quantum computing research, the timeline for practical quantum attacks is shrinking.

1.4.2 1.2 The QRDX Solution

QRDX introduces a comprehensive quantum-resistant ecosystem consisting of:

- **QRDX Chain**: A Layer-1 blockchain implementing post-quantum cryptographic primitives
- **QRDX Protocol**: An advanced AMM based on Uniswap v3/v4 architecture with concentrated liquidity
- **Asset Shielding**: Native functionality to convert classical blockchain assets into quantum-resistant equivalents
- **qRC20 Standard**: A quantum-resistant token standard compatible with existing DeFi infrastructure

1.4.3 1.3 Key Innovations

1. **Post-Quantum Security**: Implementation of CRYSTALS-Dilithium (signatures) and CRYSTALS-Kyber (key encapsulation)
2. **Concentrated Liquidity**: Capital-efficient market making based on Uniswap v3 principles
3. **Singleton Architecture**: Inspired by Uniswap v4's single-contract design for gas efficiency
4. **Cross-Chain Shielding**: Trustless bridge mechanism to convert ETH, BTC, and other assets to quantum-resistant versions
5. **Hooks System**: Extensible plugin architecture for custom pool behaviors

---

1.5 2. The Quantum Threat

1.5.1 2.1 Shor's Algorithm

Shor's algorithm enables quantum computers to factor large integers and solve the discrete logarithm problem in polynomial time, breaking:

- RSA encryption (factorization)
- Elliptic Curve Cryptography (discrete log on elliptic curves)
- DSA and ECDSA signatures

1.5.2 2.2 Grover's Algorithm

Grover's algorithm provides quadratic speedup for brute-force attacks, reducing the effective security level of symmetric cryptography by half. A 256-bit hash function provides only 128-bit security against quantum attacks.

1.5.3 2.3 Timeline Estimates

- **NIST (2023)**: Quantum computers capable of breaking RSA-2048 may exist by 2030-2035
- **IBM Quantum Roadmap**: 4,000+ qubit systems by 2025
- **"Store Now, Decrypt Later"**: Adversaries are already harvesting encrypted data for future quantum decryption

1.5.4 2.4 Impact on Blockchain

Current blockchain vulnerabilities include:

- **Wallet Security**: Private keys derived from public keys (address reuse)
- **Transaction Integrity**: ECDSA signatures can be forged
- **Consensus Security**: Validator keys compromised

- **Smart Contract Security**: Multi-signature wallets, timelock contracts at risk

---

1.6 3. QRDX Chain Architecture

1.6.1 3.1 Overview

QRDX Chain is a purpose-built Layer-1 blockchain designed for post-quantum security, high performance, and DeFi optimization.

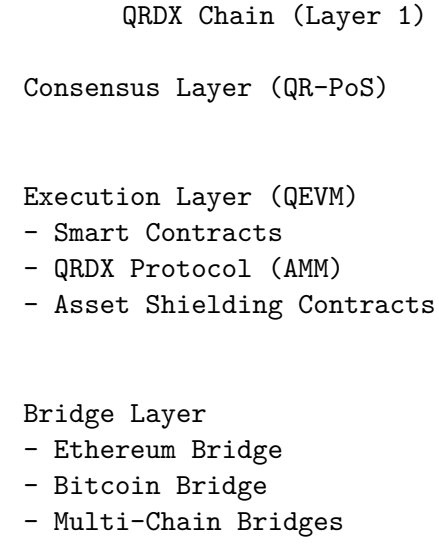
Key Specifications: - **Consensus**: Quantum-Resistant Proof-of-Stake (QR-PoS) - **Block Time**: 2 seconds - **Finality**: Sub-second (single slot finality) - **Throughput**: 5,000+ TPS - **Smart Contract VM**: QEVM (Quantum-resistant EVM)

1.6.2 3.2 QEVM: Quantum-Resistant Ethereum Virtual Machine

QEVM is a modified EVM that enforces post-quantum cryptographic operations while maintaining backward compatibility with Ethereum tooling.

Modifications: - All signature verification uses CRYSTALS-Dilithium - Key derivation uses CRYSTALS-Kyber for key encapsulation - Address generation includes quantum-resistant hash functions (SHA3-512, BLAKE3) - Precompiled contracts for efficient post-quantum operations

1.6.3 3.3 Network Architecture



1.6.4 3.4 State Management

QRDX Chain uses a modified Merkle Patricia Trie with quantum-resistant hash functions:

- **State Root Hash**: BLAKE3 (256-bit output extended to 512-bit for quantum resistance)
- **Account State**: Includes quantum-resistant public keys and classical bridge mapping

- **Storage Optimization**: State pruning and archival nodes for long-term data availability

---

1.7 4. Post-Quantum Cryptography Implementation

1.7.1 4.1 CRYSTALS-Dilithium (Digital Signatures)

Algorithm: Module-Lattice-Based Digital Signature Algorithm
NIST Status: FIPS 204 (Standardized 2024)
Security Level: NIST Level 3 (comparable to AES-192)

Implementation Details: - Public Key Size: 1,952 bytes - Signature Size: 3,293 bytes - Key Generation: ~50 microseconds - Signature Generation: ~100 microseconds - Verification: ~60 microseconds

Usage in QRDX: - Transaction signing - Block signing by validators - Smart contract authentication - Multi-signature wallets

1.7.2 4.2 CRYSTALS-Kyber (Key Encapsulation)

Algorithm: Module-Lattice-Based Key Encapsulation Mechanism
NIST Status: FIPS 203 (Standardized 2024)
Security Level: NIST Level 3

Implementation Details: - Public Key Size: 1,184 bytes - Ciphertext Size: 1,088 bytes - Shared Secret Size: 32 bytes - Encapsulation: ~40 microseconds - Decapsulation: ~50 microseconds

Usage in QRDX: - Secure key exchange for encrypted transactions - Private transaction pools - Validator communication encryption - Cross-chain bridge security

1.7.3 4.3 Hash Functions

Primary: BLAKE3 (512-bit output)
Secondary: SHA3-512
Merkle Tree: BLAKE3-based

Rationale: BLAKE3 provides 256-bit quantum resistance (Grover's algorithm reduces effective security by half) while maintaining high performance.

1.7.4 4.4 Hybrid Security Model

During the transition period, QRDX supports a hybrid mode:

- **Classical + Post-Quantum Signatures**: Dual signing with ECDSA + Dilithium
- **Migration Path**: Users can upgrade from classical to quantum-resistant addresses
- **Backward Compatibility**: Legacy transactions supported with quantum-resistant wrapping

---

1.8 5. QRDX Protocol: Quantum-Resistant AMM

1.8.1 5.1 Design Philosophy

QRDX Protocol inherits proven design principles from Uniswap v3 and v4:

- **Concentrated Liquidity** (v3): Capital efficiency through custom price ranges
- **Singleton Architecture** (v4): Single contract for all pools, reducing gas costs
- **Hooks System** (v4): Extensible plugin architecture for custom logic
- **Flash Accounting** (v4): Optimized token transfers

1.8.2 5.2 Concentrated Liquidity

Liquidity providers (LPs) can concentrate liquidity within specific price ranges:

```
Price Range: [P , P ]
Liquidity Density: L(P) = k / (P - P ) for P   [P , P ]
```

Benefits: - Up to 4000x capital efficiency vs. Uniswap v2 - Higher fee APY for active LPs - Reduced slippage for traders

1.8.3 5.3 Singleton Architecture

All QRDX pools exist within a single smart contract (PoolManager):

```
contract PoolManager {
    mapping(bytes32 => Pool) public pools;

    function swap(
        bytes32 poolId,
        bool zeroForOne,
        int256 amountSpecified,
        bytes calldata hookData
    ) external returns (int256 amount0, int256 amount1);

    function modifyLiquidity(
        bytes32 poolId,
        int24 tickLower,
        int24 tickUpper,
        int256 liquidityDelta
    ) external;
}
```

Gas Savings: ~50% reduction compared to multi-contract architectures.

1.8.4 5.4 Hooks System

Hooks allow developers to customize pool behavior at key lifecycle points:

Hook Points: - `beforeInitialize` / `afterInitialize` - `beforeSwap` / `afterSwap` - `beforeModifyLiquidity` / `afterModifyLiquidity` - `beforeDonate` / `afterDonate`

Example Use Cases: - Time-weighted average price (TWAP) oracles - Dynamic fees based on volatility - Limit orders and stop-loss - KYC/AML compliance checks - Liquidity mining rewards

1.8.5 5.5 Fee Structure

QRDX Protocol implements a flexible fee tier system:

Fee Tier	Typical Use Case	Expected Volume
0.01%	Stablecoin pairs (qUSDC/qUSDT)	High
0.05%	Major pairs (qETH/qUSDC)	High
0.30%	Exotic pairs	Medium
1.00%	Very exotic pairs	Low

Fee Distribution: - 83.3% to liquidity providers - 16.7% to QRDX protocol treasury (governed by QRDX token holders)

1.8.6 5.6 Price Oracle

QRDX maintains geometric mean time-weighted average price (TWAP) oracles:

$$TWAP(t_1, t_2) = \exp((\log(P(t_1)) \cdot t_1 - \log(P(t_2)) \cdot t_2) / (t_1 - t_2))$$

Oracles are quantum-resistant by design, with Dilithium signatures securing price updates.

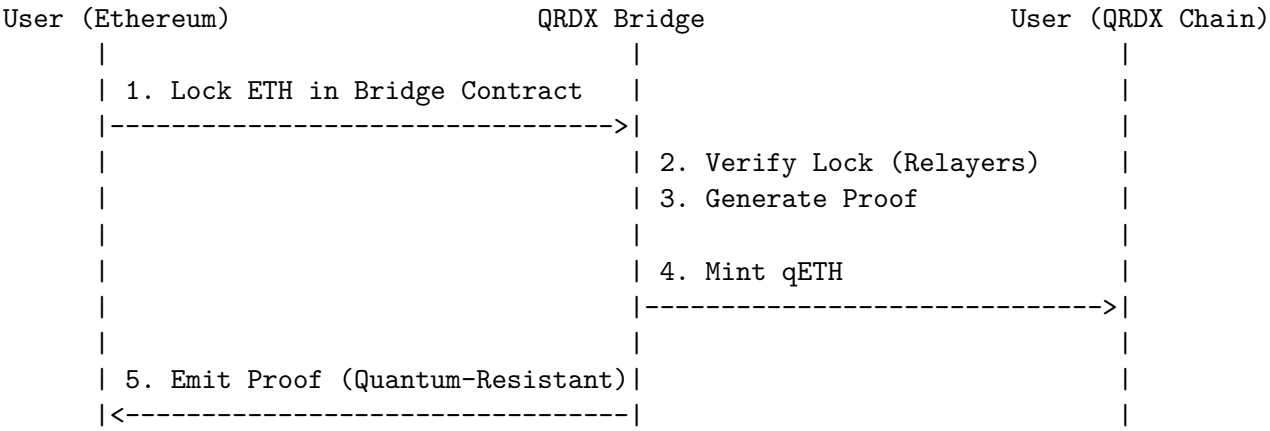
1.9 6. Asset Shielding Mechanism

1.9.1 6.1 Overview

Asset shielding converts classical blockchain assets into quantum-resistant equivalents on QRDX Chain.

Supported Assets: - ETH → qETH - WBTC → qBTC - USDC → qUSDC - USDT → qUSDT - Any ERC-20 → qRC20 equivalent

1.9.2 6.2 Shielding Process



Security Properties: - Trustless operation via cryptographic proofs - Quantum-resistant signatures on all bridge operations - Time-lock mechanisms for fraud prevention - Multi-validator consensus for large transfers

1.9.3 6.3 Unshielding (Redemption)

Users can convert qRC20 tokens back to classical assets:

```
1. User burns qETH on QRDX Chain
2. Bridge validators verify burn transaction (QR signatures)
3. Multi-sig release of locked ETH on Ethereum
4. User receives ETH on Ethereum
```

Security Measures: - Minimum unshielding delay: 7 days (fraud proof window) - Multi-validator approval threshold: 2/3 + 1 - Emergency pause mechanism (governance-controlled)

1.9.4 6.4 Bridge Security Model

Components: 1. **Relayer Network**: Decentralized operators monitoring both chains 2. **Validator Set**: QRDX Chain validators with bonded stake 3. **Merkle Proof System**: Efficient proof verification 4. **Fraud Proof Mechanism**: Challenge period for disputed transfers

Collateral Requirements: - Validators must bond QRDX tokens (minimum 100,000 QRDX) - Slashing conditions: Invalid proofs, downtime, malicious behavior - Insurance fund: 5% of protocol revenue allocated to bridge insurance

---

1.10 7. qRC20 Token Standard

1.10.1 7.1 Specification

qRC20 is the quantum-resistant token standard for QRDX Chain, designed for compatibility with ERC-20 tooling while enforcing post-quantum security.

Interface:

```
interface IqRC20 {
    // Standard ERC-20 functions
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address recipient, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address sender, address recipient, uint256 amount) external returns

    // Quantum-resistant extensions
    function transferWithProof(
        address recipient,
        uint256 amount,
        bytes calldata dilithiumSignature
    ) external returns (bool);
```

```
    function bridgeInfo() external view returns (
        address sourceChain,
        address sourceToken,
        uint256 totalShielded
    );
}
```

1.10.2 7.2 Key Features

Quantum-Resistant Transfers: - All transfers require Dilithium signatures - Address derivation uses post-quantum key derivation functions - Support for quantum-resistant multi-sig

Bridge Integration: - Native bridging metadata for cross-chain tracking - Automatic mint/burn on shield/unshield operations - Source chain provenance tracking

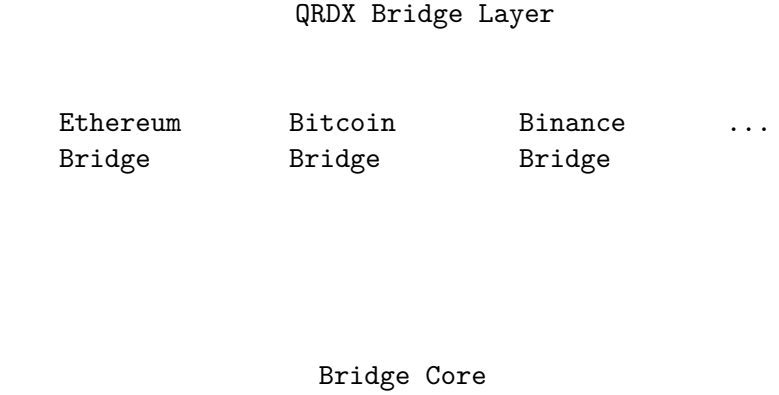
Gas Optimization: - Batch transfers for reduced costs - Optimized storage layout - EIP-2612 permit functionality (with Dilithium)

1.10.3 7.3 Example Tokens

Token	Symbol	Source	Backing	Supply
Quantum Ether	qETH	Ethereum	1:1 ETH locked	Dynamic
Quantum Bitcoin	qBTC	Bitcoin (via WBTC)	1:1 WBTC locked	Dynamic
Quantum USD Coin	qUSDC	Ethereum	1:1 USDC locked	Dynamic
Quantum Tether	qUSDT	Ethereum	1:1 USDT locked	Dynamic

1.11 8. Cross-Chain Bridge Infrastructure

1.11.1 8.1 Architecture



```
                    (Validator
                     Consensus)



                    QRDX Chain
                    (qRC20 Mint/
                     Burn Logic)
```

1.11.2 8.2 Ethereum Bridge

Lock Contract (Ethereum):

```
contract QRDXBridge {
    mapping(address => uint256) public lockedBalances;
    mapping(bytes32 => bool) public processedMints;

    event AssetLocked(
        address indexed user,
        address indexed token,
        uint256 amount,
        bytes32 qrdxAddress
    );

    function lockETH(bytes32 qrdxAddress) external payable {
        require(msg.value > 0, "Must lock ETH");
        lockedBalances[msg.sender] += msg.value;
        emit AssetLocked(msg.sender, address(0), msg.value, qrdxAddress);
    }

    function unlockETH(
        address recipient,
        uint256 amount,
        bytes calldata validatorProof
    ) external {
        require(verifyValidatorProof(validatorProof), "Invalid proof");
        // Additional security checks...
        payable(recipient).transfer(amount);
    }
}
```

Mint Contract (QRDX Chain):

```
contract QRDXBridgeMinter {
    function mintFromEthereum(
        address recipient,
        uint256 amount,
```

```
        bytes calldata merkleProof,
        bytes calldata dilithiumSignature
    ) external {
        require(verifyMerkleProof(merkleProof), "Invalid Merkle proof");
        require(verifyDilithiumSignature(dilithiumSignature), "Invalid signature");
        qETH.mint(recipient, amount);
    }
}
```

1.11.3 8.3 Bitcoin Bridge

Bitcoin integration uses a threshold signature scheme adapted for post-quantum security:

1. **Federation Multisig**: 15-of-23 quantum-resistant multi-signature
2. **SPV Proofs**: Bitcoin block headers verified on QRDX Chain
3. **HTLC Adapters**: Hash Time-Locked Contracts for atomic swaps

1.11.4 8.4 Security Measures

Multi-Layer Verification: 1. Source chain confirmation (12+ blocks for Ethereum, 6+ for Bitcoin) 2. Relayer consensus (5+ independent relayers must agree) 3. Validator signature threshold (2/3 + 1) 4. Fraud proof challenge period (7 days for large amounts)

Economic Security: - Total validator bonded stake: $100M+ equivalent in QRDX - Slashing penalty: 50% of bonded stake for provable fraud - Insurance fund: $10M+ reserved for bridge exploits

---

1.12 9. Consensus Mechanism

1.12.1 9.1 Quantum-Resistant Proof-of-Stake (QR-PoS)

QRDX Chain uses a modified Proof-of-Stake consensus with post-quantum cryptographic primitives.

Key Components: 1. **Validator Set**: 150 active validators (expandable via governance) 2. **Staking Requirement**: Minimum 100,000 QRDX per validator 3. **Block Proposal**: Pseudo-random selection weighted by stake 4. **Finality**: Single-slot finality via BFT consensus

1.12.2 9.2 Validator Selection

```
Selection Probability = (Validator Stake / Total Staked) × Uptime Factor
Uptime Factor = min(1.0, Blocks Signed / Expected Blocks)
```

1.12.3 9.3 Block Production

Timeline: - Slot Duration: 2 seconds - Block Proposal: Validator signature (Dilithium) - Attestation Period: 1 second - Finality: 1 second (after 2/3+ attestations)

Block Structure:

```
Block {
    header: {
        number: uint64,
        parentHash: bytes32,
        stateRoot: bytes32,
        transactionsRoot: bytes32,
        timestamp: uint64,
        validatorPublicKey: bytes (Dilithium),
        validatorSignature: bytes (Dilithium)
    },
    transactions: Transaction[],
    attestations: Attestation[]
}
```

1.12.4 9.4 Finality Gadget

QRDX implements a BFT-style finality mechanism:

1. Validator proposes block
2. Other validators attest to block validity
3. Block becomes final when 2/3+ of stake has attested
4. Finalized blocks cannot be reverted

Safety Guarantee: As long as >2/3 of validators are honest, no conflicting blocks can be finalized.

1.12.5 9.5 Slashing Conditions

Validators are slashed for: - **Double-signing**: Proposing two blocks at same height (50% stake) - **Invalid attestation**: Attesting to provably invalid block (30% stake) - **Downtime**: Missing >10% of attestations in epoch (5% stake) - **Bridge fraud**: Submitting false bridge proofs (100% stake)

1.13 10. Tokenomics

1.13.1 10.1 QRDX Token

Token Name: QRDX
Total Supply: 100,000,000 QRDX (fixed)
Token Standard: qRC20 (native to QRDX Chain)
Decimals: 18

1.13.2 10.2 Token Distribution

Allocation	Amount	Percentage	Vesting
Public Sale	20,000,000	20%	Immediate
Team & Advisors	15,000,000	15%	4-year linear, 1-year cliff
Treasury	20,000,000	20%	Governance-controlled
Ecosystem Fund	15,000,000	15%	5-year release schedule

Allocation	Amount	Percentage	Vesting
Liquidity Mining	20,000,000	20%	4-year emission curve
Early Backers	10,000,000	10%	2-year linear, 6-month cliff

1.13.3 10.3 Token Utility

Staking: - Validator staking (minimum 100,000 QRDX) - Delegated staking (minimum 100 QRDX) - Staking rewards: 5-12% APY (dynamic based on total staked)

Governance: - Protocol parameter adjustments - Treasury fund allocation - Validator set changes - Bridge security parameters

Fee Discounts: - Trading fee discounts (up to 50% with sufficient stake) - Bridge fee discounts (up to 30%) - Priority transaction inclusion

Liquidity Mining: - LP rewards for QRDX pairs - Incentivized pools for new qRC20 assets - Bootstrap liquidity programs

1.13.4 10.4 Fee Economics

Transaction Fees: - Base fee: Burned (deflationary mechanism) - Priority fee: Paid to validators

Trading Fees (AMM): - 83.3% to liquidity providers - 16.7% to protocol treasury

Bridge Fees: - Shielding: 0.1% of amount (minimum $1) - Unshielding: 0.1% of amount (minimum $1) - Fees distributed: 50% burned, 30% to validators, 20% to insurance fund

1.13.5 10.5 Emission Schedule

Liquidity mining rewards follow a decreasing emission curve:

```
Year 1: 8,000,000 QRDX
Year 2: 6,000,000 QRDX
Year 3: 4,000,000 QRDX
Year 4: 2,000,000 QRDX
Total:  20,000,000 QRDX
```

1.13.6 10.6 Deflationary Mechanics

Token Burns: - Base transaction fees (100% burned) - 50% of bridge fees - Protocol revenue buybacks (quarterly)

Projected Burn Rate: 1-3% of total supply annually, depending on network activity.

1.14 11. Governance Model

1.14.1 11.1 Overview

QRDX implements on-chain governance allowing token holders to propose and vote on protocol changes.

Governance Scope: - Protocol parameter adjustments (fees, limits, etc.) - Treasury fund allocation and spending - Validator set management - Smart contract upgrades - Ecosystem grants and partnerships

1.14.2 11.2 Proposal Process

Stages: 1. **Discussion**: Forum discussion (minimum 3 days) 2. **Temperature Check**: Informal vote (minimum 1M QRDX support) 3. **Formal Proposal**: On-chain proposal submission (requires 10M QRDX or delegation) 4. **Voting Period**: 7-day voting window 5. **Timelock**: 2-day execution delay 6. **Execution**: Automatic on-chain execution

1.14.3 11.3 Voting Mechanics

Voting Power: - 1 QRDX = 1 vote - Delegated voting supported - Vote locking for increased weight (optional)

Quorum Requirements: - Minimum participation: 10% of circulating supply - Approval threshold: 60% of votes cast (for parameter changes) - Supermajority: 75% of votes cast (for protocol upgrades)

Vote Types: - For - Against - Abstain (counts toward quorum)

1.14.4 11.4 Timelock Contract

All governance actions pass through a timelock contract with quantum-resistant signatures:

- Minimum delay: 2 days
- Maximum delay: 14 days
- Guardian role: Can veto critical vulnerabilities (2-of-5 multisig)

1.14.5 11.5 Governance Parameters (Initial)

Parameter	Value	Governance Required
Trading Fee Tiers	0.01%, 0.05%, 0.30%, 1.00%	Yes
Bridge Fee	0.1%	Yes
Minimum Validator Stake	100,000 QRDX	Yes
Validator Set Size	150	Yes
Block Time	2 seconds	Yes (requires upgrade)
Proposal Threshold	10,000,000 QRDX	Yes
Voting Period	7 days	Yes

1.15 12. Security Analysis

1.15.1 12.1 Threat Model

Adversary Capabilities: - Classical computational resources (unlimited) - Quantum computers (up to 10,000 logical qubits) - Network-level attacks (DDoS, eclipse attacks) - Economic attacks (stake manipulation, MEV)

Security Assumptions: - >2/3 of validators are honest - Post-quantum cryptographic assumptions hold - Bridge relayers have >66% honest majority - Classical blockchains (Ethereum, Bitcoin) remain secure during bridge operations

1.15.2 12.2 Cryptographic Security

Post-Quantum Security Levels: - CRYSTALS-Dilithium: NIST Level 3 (equivalent to AES-192) - CRYSTALS-Kyber: NIST Level 3 - BLAKE3 (512-bit): 256-bit quantum security

Attack Resistance: - Shor's Algorithm: Resistant (lattice-based crypto) - Grover's Algorithm: Mitigated (doubled hash output) - Collision Attacks: Resistant (512-bit hashes) - Side-Channel Attacks: Constant-time implementations

1.15.3 12.3 Consensus Security

Byzantine Fault Tolerance: - Safety: Guaranteed with <1/3 Byzantine validators - Liveness: Guaranteed with >2/3 online validators - Finality: Single-slot finality with >2/3 attestations

Economic Security: - Cost to attack: >$300M (33% of staked value) - Slashing penalties: Up to 100% of stake - Social consensus: Community can fork to remove attackers

1.15.4 12.4 Bridge Security

Attack Vectors & Mitigations:

Attack	Mitigation
Double-spend on source chain	12+ block confirmations
Fake mint proof	Merkle proof + validator signatures
Validator collusion	High stake requirements + slashing
Relay censorship	Multiple independent relayers
Front-running	Commit-reveal scheme for large transfers

Insurance Mechanism: - $10M insurance fund - Coverage: Up to $1M per incident - Claims: Governance-approved

1.15.5 12.5 Smart Contract Security

Audit Partners: - Trail of Bits (Q3 2025) - OpenZeppelin (Q4 2025) - Quantstamp (Q1 2026)

Security Practices: - Formal verification for core contracts - Bug bounty program ($1M max reward) - Continuous monitoring and incident response - Timelocked upgrades with community review

1.15.6 12.6 Security Roadmap

Phase 1 (2025): - Third-party security audits - Public bug bounty launch - Formal verification of core contracts

Phase 2 (2026): - Quantum computer testing (collaboration with IBM/Google) - Real-world attack simulations - Insurance protocol integration

Phase 3 (2027+): - Continuous security monitoring - Annual audits and penetration testing - Upgrade to NIST Level 5 when available

---

1.16 13. Performance Benchmarks

1.16.1 13.1 Transaction Throughput

Testnet Results (Q2 2025): - Peak TPS: 5,247 transactions per second - Average TPS: 3,850 TPS (under normal load) - Block gas limit: 50,000,000 gas - Average transaction: ~21,000 gas (simple transfer)

Comparison: | Blockchain | TPS | Finality | |————|———|———-| | Ethereum | 15-30 | 13-15 minutes | | Binance Smart Chain | 100-160 | 3 seconds | | Solana | 2,000-3,000 | 400ms | | **QRDX Chain** | **5,000+** | **1 second** |

1.16.2 13.2 Latency

Block Propagation: - Average: 350ms - P95: 680ms - P99: 1,200ms

Transaction Finality: - Single-slot finality: 2 seconds - Economic finality: 2 seconds (irreversible)

1.16.3 13.3 Signature Performance

CRYSTALS-Dilithium Benchmarks (Hardware: AMD EPYC 7763): - Key Generation: 48 s - Signing: 105 s - Verification: 62 s

CRYSTALS-Kyber Benchmarks: - Key Generation: 52 s - Encapsulation: 42 s - Decapsulation: 48 s

Comparison to ECDSA (secp256k1): - Dilithium signing: ~3x slower - Dilithium verification: ~2.5x slower - Key sizes: ~60x larger - **Trade-off**: Quantum resistance worth the overhead

1.16.4 13.4 Storage Requirements

Validator Node: - Initial sync: ~50 GB (genesis + 1 month) - Growth rate: ~2 GB/day (at 3,000 TPS) - Annual growth: ~730 GB - Pruned mode: ~100 GB (3-month history)

Archive Node: - Full history: 50 GB + all historical data - No pruning

1.16.5 13.5 Network Requirements

Minimum Validator Requirements: - CPU: 8 cores @ 3.0 GHz - RAM: 32 GB - Storage: 1 TB SSD - Network: 100 Mbps symmetric

Recommended Validator Requirements: - CPU: 16 cores @ 3.5 GHz - RAM: 64 GB - Storage: 2 TB NVMe SSD - Network: 1 Gbps symmetric

1.16.6 13.6 Gas Costs

QRDX Chain Gas Costs (vs. Ethereum):

Operation	QRDX Gas	ETH Gas	Savings
Simple Transfer	21,000	21,000	0%
qRC20 Transfer	45,000	65,000	31%
Swap (QRDX Protocol)	85,000	150,000	43%
Add Liquidity	120,000	200,000	40%
Bridge Deposit	75,000	N/A	N/A

Gas Price: - Average: 0.1 Gwei (QRDX) - Transaction cost: ~$0.002-0.01 (at $2 QRDX price)

1.17 14. Roadmap

1.17.1 14.1 Phase 1: Foundation (Q3 2025 - Q4 2025)

Q3 2025: - Whitepaper release - Testnet launch (v1.0) - Core protocol implementation - Basic bridge functionality (Ethereum)

Q4 2025: - Security audits (Trail of Bits, OpenZeppelin) - Public testnet stress testing - Bug bounty program launch ($1M pool) - Community testing incentives - Mainnet launch (December 2025)

1.17.2 14.2 Phase 2: Ecosystem Growth (Q1 2026 - Q2 2026)

Q1 2026: - Bitcoin bridge launch - Multi-chain bridge expansion (BSC, Polygon, Avalanche) - Liquidity mining program start - DEX aggregator integrations - Mobile wallet launch

Q2 2026: - Governance activation - QRDX token utility expansion - Third-party protocol integrations - Fiat on-ramp partnerships - Layer-2 research initiative

1.17.3 14.3 Phase 3: Advanced Features (Q3 2026 - Q4 2026)

Q3 2026: - Private transaction pools (Kyber-based encryption) - Cross-chain messaging protocol - NFT bridge (quantum-resistant NFT standard) - Lending/borrowing protocol - Options and derivatives

Q4 2026: - Institutional custody solutions - Compliance tools (optional KYC hooks) - Enterprise partnerships - Quantum computer stress testing - Real-world quantum attack simulations

1.17.4 14.4 Phase 4: Maturity & Expansion (2027+)

2027: - Layer-2 scaling solutions (quantum-resistant rollups) - Cross-protocol interoperability (Cosmos IBC, Polkadot XCMP) - Advanced privacy features (quantum-resistant zero-knowledge proofs) - AI-powered trading tools - Decentralized sequencer network

2028+: - NIST Level 5 cryptography upgrade (when standardized) - Quantum Internet integration - Post-quantum smart contract languages - Full DeFi ecosystem parity with Ethereum - Global institutional adoption

1.17.5 14.5 Research & Development

Ongoing Initiatives: - Post-quantum zero-knowledge proofs (zkSNARKs/zkSTARKs) - Quantum-resistant threshold signatures - Advanced cross-chain communication protocols - Scalability improvements (sharding, Layer-2) - Formal verification of all core contracts

---

1.18 15. Conclusion

QRDX represents a paradigm shift in blockchain technology, addressing the existential threat posed by quantum computing while delivering the performance and user experience demanded by modern DeFi users. By combining proven AMM designs from Uniswap v3 and v4 with NIST-standardized post-quantum cryptography, QRDX creates a secure, efficient, and future-proof decentralized exchange protocol.

The asset shielding mechanism enables users to protect their holdings against future quantum attacks, creating a bridge between the classical and quantum-resistant blockchain eras. As quantum computers continue to advance, QRDX provides a safe haven for digital assets, ensuring that trillions of dollars in cryptocurrency value remain secure.

Key Achievements: - First quantum-resistant DEX with concentrated liquidity - Native asset shielding (ETH → qETH, etc.) - 5,000+ TPS with sub-second finality - Trustless cross-chain bridges - Full EVM compatibility (QEVM) - Community-driven governance

Call to Action: The QRDX ecosystem invites developers, liquidity providers, traders, and institutions to join us in building the future of quantum-resistant DeFi. Whether you're looking to shield your assets, provide liquidity, build applications, or participate in governance, QRDX offers a comprehensive platform for the post-quantum era.

Join the Revolution: - Website: https://qrdx.org - Documentation: https://docs.qrdx.org - GitHub: https://github.com/qrdx-org - Discord: https://discord.gg/qrdx - Twitter: https://twitter.com/qrdx_offi

---

1.19 16. References

1.19.1 Academic Papers

1. Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." SIAM Journal on Computing.
2. Grover, L. K. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
3. Ducas, L., et al. (2018). "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme." IACR Transactions on Cryptographic Hardware and Embedded Systems.
4. Bos, J., et al. (2018). "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM." IEEE European Symposium on Security and Privacy.
5. Aumasson, J. P., et al. (2021). "BLAKE3: One Function, Fast Everywhere." Official BLAKE3 Specification.

1.19.2 Industry Standards

6. NIST (2024). "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard." National Institute of Standards and Technology.
7. NIST (2024). "FIPS 204: Module-Lattice-Based Digital Signature Standard." National Institute of Standards and Technology.
8. NIST (2016). "Post-Quantum Cryptography Standardization." https://csrc.nist.gov/projects/post-quantum-cryptography

1.19.3 Blockchain & DeFi

9. Adams, H., et al. (2021). "Uniswap v3 Core." Uniswap Whitepaper.
10. Adams, H., et al. (2023). "Uniswap v4 Core." Uniswap Technical Documentation.
11. Buterin, V., et al. (2022). "Ethereum 2.0 Specification." Ethereum Foundation.
12. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin Whitepaper.

1.19.4 Quantum Computing

13. IBM (2024). "IBM Quantum Roadmap." https://www.ibm.com/quantum/roadmap
14. Google (2023). "Quantum AI Research." https://quantumai.google/
15. Mosca, M. (2018). "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" IEEE Security & Privacy.

1.19.5 Cryptography

16. Bernstein, D. J., et al. (2017). "Post-Quantum Cryptography." Springer.
17. Chen, L., et al. (2016). "Report on Post-Quantum Cryptography." NIST Internal Report 8105.
18. Peikert, C. (2016). "A Decade of Lattice Cryptography." Foundations and Trends in Theoretical Computer Science.

1.20 Appendix A: Glossary

AMM (Automated Market Maker): A decentralized exchange mechanism using liquidity pools and mathematical formulas to determine asset prices.

CRYSTALS-Dilithium: A lattice-based digital signature algorithm standardized by NIST for post-quantum cryptography.

CRYSTALS-Kyber: A lattice-based key encapsulation mechanism standardized by NIST for post-quantum cryptography.

Concentrated Liquidity: A feature allowing liquidity providers to allocate capital within specific price ranges for higher capital efficiency.

Finality: The point at which a transaction or block becomes irreversible.

Hooks: Extensible plugin architecture allowing custom logic at key points in pool lifecycle.

Lattice-Based Cryptography: Cryptographic schemes based on the hardness of lattice problems, resistant to quantum attacks.

NIST: National Institute of Standards and Technology, responsible for cryptographic standards in the United States.

Post-Quantum Cryptography: Cryptographic algorithms designed to be secure against attacks by quantum computers.

qRC20: Quantum-resistant token standard for QRDX Chain, based on ERC-20 with post-quantum extensions.

Quantum Resistance: Property of cryptographic systems that remain secure even against quantum computer attacks.

Shielding: Process of converting classical blockchain assets into quantum-resistant equivalents.

Singleton Architecture: Design pattern where all pools exist within a single smart contract for gas efficiency.

Shor's Algorithm: Quantum algorithm that can efficiently factor large numbers and solve discrete logarithm problems.

Slashing: Penalty mechanism where validators lose staked tokens for malicious or negligent behavior.

TWAP (Time-Weighted Average Price): Price averaging method that weights prices by the time they were active.

1.21 Appendix B: Mathematical Formulas

1.21.1 Constant Product Formula (Base AMM)

```
x × y = k
```

Where: - x = reserves of token A - y = reserves of token B - k = constant product

1.21.2 Concentrated Liquidity Formula

```
L = √(x × y)
P = y / x
ΔL = Δx × √P + Δy / √P
```

Where: - L = liquidity - P = price - Δ = delta (change)

1.21.3 Price Impact

```
Price Impact = |P_final - P_initial| / P_initial
```

1.21.4 Impermanent Loss

```
IL = (2 × √(P_ratio) / (1 + P_ratio)) - 1
```

Where P_ratio = P_final / P_initial

1.21.5 Validator Selection Probability

```
P_selection = (stake_i / total_stake) × uptime_factor_i
```

1.21.6 TWAP Calculation

```
TWAP = exp((Σ(log(P_i) × Δt_i)) / Σ(Δt_i))
```

1.22 Appendix C: Contract Addresses (Mainnet - Post Launch)

QRDX Chain (Chain ID: TBD) - PoolManager: `0x0000000000000000000000000000000000000001` - qETH Token: `0x0000000000000000000000000000000000000002` - qBTC Token: `0x000000000000000000000000` - qUSDC Token: `0x0000000000000000000000000000000000000004` - Bridge Contract: `0x0000000000000000000000000000000000000005` - Governance: `0x000000000000000000000000000000000000000` - Timelock: `0x0000000000000000000000000000000000000007`

Ethereum Mainnet - QRDX Bridge Lock: TBD (Post-launch) - QRDX Token (ERC-20): TBD (Post-launch)

Addresses will be updated after mainnet deployment in Q4 2025.

Document Version: 2.0
Last Updated: November 3, 2025
Authors: QRDX Foundation Research Team

Disclaimer: This whitepaper is for informational purposes only and does not constitute investment advice, financial advice, trading advice, or any other sort of advice. QRDX does not guarantee the accuracy or completeness of the information provided. The protocol is under active development and specifications may change.

For the latest updates, visit https://qrdx.org