QANT

A Next-Generation Platform for Secure Digital Assets

Version 1.0

© 2025 QANT Team

Table of Contents

Executive Summary

QANT represents a paradigm shift in blockchain security, introducing the first comprehensive quantum-resistant cryptocurrency platform with selectable privacy levels. Built upon advanced post-quantum cryptographic primitives, QANT addresses the critical vulnerability that threatens all existing blockchain systems: the advent of quantum computing.

The Quantum Threat

Current cryptographic systems rely on Elliptic Curve Cryptography (ECC) and RSA, which are vulnerable to quantum attacks. Shor's algorithm can break these systems in polynomial time when executed on a sufficiently powerful quantum computer. QANT mitigates this existential risk by implementing lattice-based cryptography which remains secure against both classical and quantum adversaries.

Privacy by Design

Unlike other privacy-focused cryptocurrencies, QANT offers three distinct privacy modes: transparent, fully private, and private with accountability. This flexibility enables users to choose the appropriate level of privacy for their use case while maintaining regulatory compliance when necessary.

Vision and Objectives

QANT aims to establish a future-proof blockchain infrastructure that balances security, privacy, and regulatory compliance.

1. Quantum Resistance

QANT employs Module-LWE (Learning With Errors) and Module-SIS (Short Integer Solution) primitives to safeguard against quantum attacks. These lattice-based cryptographic schemes have been extensively studied by the cryptographic community and are recommended by NIST for post-quantum security. Unlike traditional systems that may require hard forks to upgrade cryptography, QANT is quantum-safe from inception.

2. Multi-Tier Privacy

The platform supports three privacy levels:

- Basic Privacy: Transparent transaction data with one-time wallet addresses (similar to Bitcoin)
- Full Privacy: Hidden addresses and encrypted transaction values using homomorphic commitments
- Full Privacy with Accountability: Private to all except authorized auditors/regulators via verifiable encryption

This tiered approach allows individuals, enterprises, and institutions to select privacy levels appropriate to their operational requirements and regulatory obligations.

3. Regulatory Compliance

The DAPOA (Decentralized Anonymous Payment with Optional Accountability) framework enables selective disclosure of transaction details to designated authorities. This capability ensures QANT can meet Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements while preserving user anonymity from unauthorized parties.

Technical Architecture

QANT's architecture is built upon rigorous cryptographic foundations, ensuring both security and privacy guarantees.

Cryptographic Foundations

• Lattice-based Signatures: ML-DSA (Module-Lattice Digital Signature Algorithm) for quantum-resistant transaction authentication

• Homomorphic Commitments: Pedersen commitments enable encrypted amount storage while preserving verifiability

• Zero-Knowledge Range Proofs: Bulletproofs ensure transaction values remain within valid bounds without revealing amounts

• Linkable Ring Signatures: Provides unlinkability between transactions while preventing double-spending

• Verifiable Encryption: Enables selective disclosure for accountability without compromising general privacy

Data Model

The blockchain supports three transaction output types:

Public TXOs: Fully transparent, similar to Bitcoin UTXOs, suitable for public auditing and transparent ledgers.

Value-Hidden TXOs: Transaction amounts are encrypted using homomorphic commitments, while addresses remain visible. This provides amount privacy while maintaining auditability.

Private TXOs: Both addresses and amounts are hidden using linkable ring signatures and commitments, providing maximum privacy.

Transaction Types

QANT supports four transaction types:

1. Public Transaction: Standard transparent transaction
2. Mask Transaction: Converts public funds to private state
3. Private Transaction: Transfers between private states
4. Unmask Transaction: Converts private funds to public state

Consensus Mechanism

QANT launches with Proof-of-Work (PoW) consensus to ensure decentralization and security. The roadmap includes a planned transition to Proof-of-Stake (PoS) to improve energy efficiency while maintaining security guarantees through lattice-based staking mechanisms.

DAPOA Framework

The Decentralized Anonymous Payment with Optional Accountability (DAPOA) model forms the core privacy architecture of QANT.

Core Properties

Anonymity: Complete sender/receiver unlinkability through linkable ring signatures. Even with access to the full blockchain, transactions cannot be traced to specific participants.

Value Hiding: Transaction amounts are encrypted using homomorphic commitments, preventing amount inference through blockchain analysis.

Consumed Coin Hiding: Input-output unlinkability ensures that spent coins cannot be connected to newly created outputs, preventing transaction graph analysis.

Selective Disclosure

Optional Accountability: Tracking keys enable designated authorities (regulators, auditors) to decrypt transactions may embed a tracking public key that enables controlled accountability. When combined with verifiable encryption, authorized parties can decrypt transaction details to prove compliance without requiring access to private keys or compromising general anonymity. This selective disclosure mechanism satisfies regulatory requirements for financial transparency while preserving user privacy.

Security Guarantees

DAPOA provides provable security guarantees:

- Computational anonymity against polynomial-time adversaries
- Statistical privacy guarantees for honest users
- Selective traceability only with proper authorization
- Double-spending prevention through linkable ring signatures

Privacy Architecture

QANT's modular privacy system allows users to select appropriate privacy levels based on their needs.

Privacy Mode Selection

Users can switch between privacy modes at any time through mask/unmask transactions. This flexibility enables:

- Public verification for transparent operations
- Amount privacy for commercial confidentiality
- Full privacy for personal financial transactions
- Regulated privacy for institutional compliance

Implementation Details

The privacy architecture is implemented through:

Ring Signatures: Each private transaction includes a ring of possible senders, making it computationally infeasible to identify the actual sender. The linkability property prevents double-spending while maintaining anonymity.

Stealth Addresses: Receivers generate one-time addresses for each transaction, preventing address reuse and transaction clustering.

Commitment Schemes: Homomorphic commitments allow transaction verification without revealing amounts, enabling zero-knowledge proofs of transaction validity.

Performance Considerations

Privacy comes with computational and storage costs. QANT optimizes these through:

- Efficient lattice-based cryptography with smaller key sizes
- Bulletproofs for compact zero-knowledge proofs
- Ring signature optimizations reducing signature sizes
- Optional privacy modes allowing users to balance privacy and efficiency

Tokenomics

QANT (QNT) token economics are designed to support long-term sustainability and ecosystem growth.

Supply Model

QNT implements a capped supply model with a maximum of 21 million tokens, ensuring scarcity and value preservation. The supply schedule is designed to incentivize early adoption while maintaining long-term economic stability.

Distribution

Token distribution is structured as follows:

• 60% Mining/Staking Rewards: Distributed to network validators and stakers to incentivize security and participation

• 20% Ecosystem Development: Reserved for grants, partnerships, and ecosystem growth initiatives

• 10% Partnerships & R&D: Allocated for strategic partnerships and continued research and development

• 10% Team & Advisors: Subject to multi-year vesting schedules to align long-term interests

Token Utility

QNT serves multiple functions within the ecosystem:

• Governance: Token holders can propose and vote on protocol upgrades and parameter changes

• Staking: Users stake QNT to secure the network and earn rewards

• Transaction Fees: QNT is used to pay network transaction fees

• Ecosystem Services: Required for premium features and services within the QANT ecosystem

Economic Model

The economic model balances security incentives, user adoption, and long-term sustainability. Staking rewards decrease over time to encourage early participation while maintaining network security. Transaction fees provide ongoing network funding beyond the initial distribution period.

Development Roadmap

QANT's development follows a structured roadmap ensuring gradual rollout of features and security.

Phase 1: Q1–Q2 2026 - Foundation

• Completion of QANT Framework v1.0 whitepaper
• Finalization of cryptographic primitives and security proofs
• Core protocol specification and architecture documentation
• Initial codebase development and security audits
• Community building and early adopter programs

Phase 2: Q3 2026 - Testnet Launch

• Public testnet deployment with quantum-safe cryptography
• Quantum-safe wallet development and testing
• Private transaction implementation and testing
• Community testing and feedback collection
• Performance optimization and scalability improvements

Phase 3: Q1 2027 - Mainnet Beta

• Mainnet beta launch with restricted token distribution
• DAPOA privacy integration and accountability features
• Exchange partnerships and liquidity provision
• Enterprise pilot programs
• Comprehensive security audits and penetration testing

Phase 4: Q3 2027 - Governance Launch

• Transition to stake-based consensus mechanism
• Governance system activation
• Full mainnet launch with public token distribution
• Institutional adoption programs
• Regulatory compliance certification

Phase 5: 2028+ - Expansion

• Sidechain development for scalability
• Smart contract platform integration
• Web3 and DeFi ecosystem integration
• Cross-chain interoperability protocols
• Continued research and quantum threat monitoring

Conclusion

QANT establishes a secure, quantum-resistant, and privacy-flexible ecosystem built for the coming era of decentralized finance. By combining post-quantum cryptography with a modular privacy framework, QANT offers both individuals and institutions a resilient foundation for secure digital value exchange.

Key Advantages

QANT differentiates itself through:

- Quantum Resistance: Protection against future quantum computing threats
- Flexible Privacy: Three privacy modes suitable for different use cases
- Regulatory Compliance: Accountability features for institutional adoption
- Provable Security: Rigorous cryptographic foundations with formal proofs
- Scalability: Architecture designed for future growth and expansion

Vision for the Future

As quantum computing capabilities advance, traditional blockchain systems face existential security risks. QANT proactively addresses this challenge by implementing quantum-resistant cryptography from the ground up. The platform's flexible privacy architecture ensures it can serve diverse needs—from individuals seeking financial privacy to institutions requiring regulatory compliance.

Join the Revolution

QANT invites researchers, developers, and users to participate in building the quantum-resistant future of blockchain technology. Together, we can create a secure, private, and compliant infrastructure for digital value exchange.

By combining cutting-edge cryptographic research with practical blockchain engineering, QANT positions itself as the secure foundation for the next generation of decentralized applications and financial systems.

For more information, visit qant.org or contact the team at info@qant.org