Q-NarwhalKnight Announcement

To: cryptography@metzdowd.com **From:** Q-NarwhalKnight Development Team **Subject:** Q-NarwhalKnight: A Private, Post-Quantum Peer-to-Peer Electronic Cash System **Date:** December 2025

I've developed a new electronic cash system that is:

- **Fully peer-to-peer** – no trusted third party
- **Completely private** – permissioned access, encrypted by default
- **Quantum-resistant** – built for the post-quantum cryptographic era

---

PRIVACY BY DESIGN

Unlike public blockchains where every transaction is visible to the world, Q-NarwhalKnight is a **private blockchain** with:

Feature	Description
End-to-end encryption	All network traffic encrypted via Noise protocol
Zero-knowledge proofs	Transaction validation without data exposure
Tor integration	Dedicated circuits per validator, IP obfuscation
Dandelion++ gossip	Traffic analysis resistance built into consensus
Private mempool	Transactions invisible until block inclusion

Your financial activity is **yours alone**.

TECHNICAL SPECIFICATIONS

Property	Value
Consensus	DAG-BFT (Byzantine Fault Tolerant)
Finality	Sub-50 milliseconds
Throughput	48,000+ TPS theoretical maximum
Signatures	CRYSTALS-Dilithium5 (post-quantum)
Key Exchange	Kyber1024 (NIST PQC standard)
Block Structure	Multi-parent DAG (no orphan waste)

POST-QUANTUM SECURITY

The cryptographic foundation assumes quantum adversaries exist **today**:

Phase 1 (Active)

- Dilithium5 signatures (NIST FIPS 204)
- Kyber1024 key encapsulation (NIST FIPS 203)
- AEGIS-QL authenticated encryption
- SHA3-256 block integrity

Phase 2 (Planned)

- Quantum Key Distribution preparation
- Hybrid classical+PQ mode for transition

NETWORK ARCHITECTURE

PRIVATE NETWORK

- Permissioned node participation
- Encrypted P2P via libp2p + Noise
- Kademlia DHT for private peer discovery
- Gossipsub with authenticated topics
- No public block explorers
- No third-party API access

Bootstrap (private testnet):

`/ip4/185.182.185.227/tcp/9001/p2p/12D3KooWQbKp6RYgZpC3dUCYou5LrVmd7pFa74rQj7rsK1sWUnfu`

WHITEPAPER

Available at: **quillon.xyz/whitepaper**

NODE SOFTWARE

Private access only. Contact for authorization.

```
# Authorized users only
wget https://quillon.xyz/downloads/q-api-server-v2.3.11
chmod +x q-api-server-v2.3.11
```

WHY PRIVATE?

Public blockchains have failed the promise of financial privacy:

1. **Chain analysis firms** track every transaction
2. **Governments demand** exchange KYC/AML data
3. **Employers, insurers, landlords** screen blockchain history
4. **Front-running bots** exploit public mempool visibility

A private blockchain with post-quantum cryptography is the only path forward for those who believe financial privacy is a human right.

THREAT MODEL

We assume:

- Nation-state adversaries with quantum computing capability
- Global passive adversaries monitoring network traffic
- Active attackers attempting Sybil/eclipse attacks

- Sophisticated chain analysis attempting deanonymization

The system is designed to resist all of the above.

OPEN FOR TECHNICAL REVIEW

I welcome feedback on:

- VDF-based anchor election mechanism
- Post-quantum signature aggregation efficiency
- Privacy/performance tradeoffs in Tor integration
- DAG consensus security assumptions

Source code available for authorized security researchers.

DISCLAIMER

This is experimental software. Private network. Invitation only.

"Privacy is not about having something to hide. Privacy is about having something to protect."

HISTORICAL CONTEXT

This announcement follows in the tradition of Satoshi Nakamoto's original Bitcoin announcement to the Metzdowd cryptography mailing list on October 31, 2008. However, Q-NarwhalKnight represents a fundamentally different approach:

Aspect	Bitcoin (2008)	Q-NarwhalKnight (2025)
Privacy	Pseudonymous (public ledger)	Private (encrypted ledger)
Consensus	Proof of Work	DAG-BFT with VDF anchoring
Finality	60 minutes (6 confirmations)	Less than 50 milliseconds
Quantum Security	None (ECDSA vulnerable)	Dilithium5 + Kyber1024
Throughput	7 TPS	48,000+ TPS
Network	Public, permissionless	Private, permissioned

The threat landscape has evolved. So must our tools.

CONTACT

- Website: quillon.xyz
- Network: testnet-phase16
- Protocol: Q-NarwhalKnight v2.3.11

End of document