ETSI/IQC Quantum Safe Cryptography Conference 2026

Migration to quantum safe blockchains

Presented by:

Michel Barbeau, Carleton University. Randy Kuang, Quantropi Inc.

17/06/2026

Quantum Threat to Blockchain Cryptography

- Classical blockchains rely on ECDSA, Ed25519, ECDH
- Shor's algorithm breaks them with large-scale quantum computers
- "Harvest now, decrypt later": encrypted data recorded today can be decrypted later
- **Important nuance:** Signatures are *not* retroactively decrypted (no historic fund theft), but an adversary with a quantum computer could forge signatures in real time to hijack live accounts.
- For blockchains using **confidential transactions or off-chain channels** (KEMs), harvest-now is an immediate, catastrophic risk.
- NIST lattice standards: Kyber (KEM), Dilithium (signatures) – but large keys/signatures cause scalability issues.

Proposed Cryptographic Primitives

MPPK KEM – Key Encapsulation

- Hidden-ring multivariate polynomials over $\mathrm{GF}(p)$, $\mathbb{Z}/t\mathbb{Z}$
- Linear config ($\lambda = 1$) $\rightarrow$ no root-finding, high speed
- **Security:** IND-CPA (modular Diophantine hardness)
- **Sizes (NIST V):** PK 350 B, CT 350 B
- **Performance:** $16k$–$22k$ CPU cycles (encap/decap)

HPPK DS – Digital Signature

- Extends MPPK with Barrett reduction masking
- Deterministic $\rightarrow$ no transaction malleability
- **Security:** EUF-CMA (exponential best attacks)
- **Sizes (NIST V):** PK 356 B, signature 272 B
- **Performance:** sign $\approx 16k$, verify $\approx 22k$ cycles

Both primitives are **quantum-safe** (no known polynomial-time quantum attacks) and form the *sole* public-key layer of our blockchain architecture.

Comparison With Lattice Candidates

Table 1: Public key and signature/ciphertext sizes at NIST Level V (bytes)

Scheme	Public key	Signature / Ciphertext
Dilithium5	1,600	3,293
Kyber1024	1,568	1,568 (ciphertext)
HPPK DS (Level V)	356	272
MPPK KEM (Level V)	350	350 (ciphertext)

- Dilithium signatures >3 KB $\rightarrow$ 1 MB block holds only 300 transactions; HPPK: 4,000 transactions (order-of-magnitude improvement)
- On-chain state bloat: In state-based blockchains (e.g., Ethereum), validator nodes store all public keys permanently. Moving from 32-byte classical keys to 1,600-byte Dilithium keys causes exponential storage replication over millions of accounts. Our 356-byte public keys mitigate this explosion.
- Lattice: discrete security levels; multivariate: continuous trade-off via p, m

Quantum-Safe Blockchain Architecture

Core Principle
Native, exclusive use of **MPPK KEM** and **HPPK DS** – no other public-key primitives.

- **Compactness:** HPPK signatures as small as 272 bytes (Level V) – 10× smaller than Dilithium.
- **Quantum safety:** Security rests on multivariate polynomial hardness (no known quantum speedup).
- **Consensus agnostic:** Works with PoW, PoS, or any standard protocol – decoupled layer.

Account Model:

$$\text{Address} = \text{SHA256}(\text{HPPK\_PK} \parallel \text{MPPK\_PK})$$

- One address binds both signature and encryption keys
- **Security:** Collision resistance – 128-bit post-quantum (Grover). Pre-image resistance – 256 bits classically / 128 bits under Grover (still sufficient).
- Optional upgrade to SHA-3 for higher margin

Transaction and Block Structure

Transaction T – compact and self-contained:

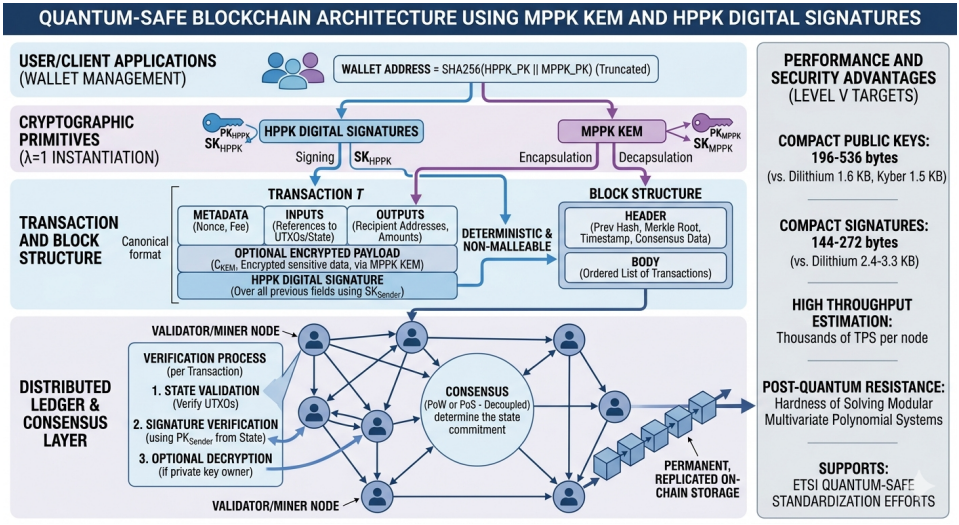
1. **Metadata:** version, nonce, fee
2. **Inputs:** UTXOs or account state references
3. **Outputs:** recipient addresses + amounts
4. **Encrypted payload (optional):** MPPK KEM ciphertext $\|$ AES-GCM encrypted data
5. **Signature:** HPPK DS over all preceding fields (deterministic $\rightarrow$ no malleability)

Block:

- Header: previous hash, Merkle root, timestamp, consensus data, state commitment
- Body: ordered list of validated transactions

No extra crypto primitives – minimal, uniform footprint.

Architecture Overview Diagram



The diagram illustrates the complete flow: user wallets, transaction assembly, verification, consensus,

Confidential Transactions – Optional, Lightweight

How it works:

1. Sender retrieves recipient's **MPPK public key**
2. Encapsulates random symmetric key K using MPPK KEM $\rightarrow C_{\mathrm{KEM}}$
3. Encrypts sensitive payload (amount, memo, etc.) with K (AES-GCM)
4. Transaction includes C_{KEM} and ciphertext

What this provides (and does not provide)

- **Provides:** Data / memo confidentiality for point-to-point secure communication (e.g., hidden contract parameters, private metadata).
- **Does not provide:** Public validation of masked balances (that would require zero-knowledge proofs like Bulletproofs). Our architecture focuses on compact, quantum-safe *optional* confidentiality, not full private transaction validation.
- MPPK KEM is IND-CPA secure, no heavy ZK overhead.

Confidentiality is optional – transactions without encrypted payload are fully public.

Migration Path Toward ETSI Standardization

- ETSI has initiated work on post-quantum migration strategies for distributed ledgers.
- Our architecture illustrates a concrete design using compact multivariate primitives.
- Standalone blockchain – backward compatibility not assumed.
- Bridge mechanism: lock assets on legacy chain, mint on quantum-safe chain, authenticate via HPPK DS signatures.

This work aims to serve as an input to ongoing ETSI discussions on quantum-safe blockchains.

Conclusion

- Proposed a quantum-safe blockchain based on MPPK KEM and HPPK DS.
- Compact sizes: public keys 196–536 bytes, signatures 144–272 bytes.
- Performance: tens of thousands of cycles per operation; high throughput possible.
- Optional confidentiality via MPPK KEM.
- Acknowledgment: MPPK/HPPK not yet as widely cryptanalyzed as NIST lattice schemes – further analysis needed.
- Hoped to motivate additional research and standardization.

Thank you!

References

- NIST IR 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, 2022.
- R. Kuang, M. Perepechaenko, M. Barbeau, *A new post-quantum multivariate polynomial public key encapsulation algorithm*, Quantum Information Processing, 21, 360 (2022).
- R. Kuang, M. Perepechaenko, R. Toth, M. Barbeau, *Benchmark Performance of the Multivariate Polynomial Public Key Encapsulation Mechanism*, in: Risks and Security of Internet and Systems, Springer, 2023, pp. 239–255.
- R. Kuang, M. Perepechaenko, M. Sayed, D. Lou, *Homomorphic polynomial public key with Barrett transformation for digital signature*, Academia Quantum, 1 (2024).
- S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008.
- G. Wood, *Ethereum: A secure decentralised generalised transaction ledger*, 2014.