UTON QUANTUM BLOCKCHAIN

Whitepaper

October 09, 2025

Summary

UTON Quantum Blockchain (UQB) is a next-generation, quantum-secure public blockchain (Layer-1) designed to withstand both classical and quantum adversaries.

Built upon a Tendermint-BFT foundation and fully compatible with the Ethereum Virtual Machine (EVM), UQB integrates post-quantum cryptography (PQC) natively across all layers — from accounts and consensus to networking and storage.

Its mission is clear: to future-proof digital assets, smart contracts, and decentralized applications against the coming quantum era. UQB replaces vulnerable elliptic-curve and RSA-based cryptography with NIST-standardized algorithms such as CRYSTALS-Dilithium, CRYSTALS-Kyber, and SPHINCS+, ensuring verifiable security for decades.

Beyond security, UQB emphasizes performance, scalability, and compliance, achieving deterministic low latency, eco-efficient Proof-of-Stake (PoS), and audit-ready architecture. UTN — the network’ s native token — powers gas, staking, governance, and security assurance.

Through a certification-first approach, UQB aims to become the world’ s first formally audited and PQ-certified blockchain, setting a new benchmark for institutional-grade Web3 infrastructure.

1. Overview

UTON QUANTUM BLOCKCHAIN (UQB) is a Tendermint-BFT–derived, EVM-compatible Layer-1 chain re-architected for the quantum era.

It introduces hybrid and quantum-only security modes for accounts and validators, post-quantum handshakes for P2P, and precompiled PQC primitives for smart contracts.

1.1 Core tenets

- **Quantum-grade security end-to-end:** Keys, handshakes, signatures, and state proofs use PQC (e.g., ML-DSA / SPHINCS+ for signatures; ML-KEM for key establishment), with classical algorithms supported only for backward compatibility and phased out via governance.

- **EVM compatibility without compromises:** Full Solidity support plus new PQ precompiles for verification and key encapsulation, enabling dApps to adopt PQC without custom cryptography code.
- **Deterministic performance & low fees:** Batched PQ verification, bitmap-based vote commitments, and optimized state proofs maintain low latency and predictable gas.
- **Certification-first design:** Architecture and implementations are organized around conformance with PQC standards (e.g., FIPS-grade PQ suites) and security evaluation baselines (e.g., ISO/IEC 15408/Common Criteria levels where applicable).
- **Investor value:** UQB positions UTN as a long-duration asset by eliminating cyber attacks , crypto hacking and harvest-now-decrypt-later risk on chain state and user assets, opening regulated markets that will mandate quantum-safe rails.

1.2 Why now

Quantum computing timelines are uncertain, but data and signatures published today remain valuable for decades.
Attackers can harvest ledgers now and verify or forge later when quantum capabilities mature.
UQB makes that strategy economically and cryptographically unviable—protecting keys, transactions, and historical state forever.

1.3 Key features and benefits

- Strongest-available cryptography with hybrid and pure-PQC modes
- Rich scalability via Tendermint-BFT optimizations and PQ-aware batching

- Fast, low-cost finality with per-block PQ signature batching and vote compression
- Eco-efficient PoS with deterministic BFT and low hardware overhead
- EVM + PQC: seamless dev experience; legacy dApps can opt-in gradually

2. Account Model

UQB preserves the familiar state-based account model but introduces quantum-ready account classes and address derivation compatible with PQ public keys.

2.1 User Account

2.1.1 Account classes

- **Q-Hybrid Account (QHA):** Holds both an ECDSA (secp256k1) keypair and a PQ signature keypair (default ML-DSA; SPHINCS+ optional). Transactions are signed with a hybrid signature (ECDSA + PQ) during the transition period.
- **Q-Native Account (QNA):** Pure PQ signature only (ML-DSA or SPHINCS+). Recommended for new users and institutions after the deprecation period begins.
- **Multisig / Threshold PQ Accounts:** N-of-M aggregation at the application layer using PQ signatures, with on-chain validation via PQ precompiles.

2.1.2 Addresses

- Addresses are derived from SHA3-256/SHAKE256 digests of canonicalized PQ public keys (or hybrid bundles) truncated to 20 bytes for EVM compatibility.

- Optional 32-byte “extended address” format is supported at the JSON-RPC level for PQ-native apps.

2.1.3 Security properties

- Nonce semantics unchanged; replay protection and ordering preserved.
- Key rotation supports seamless migration from hybrid to PQ-native by governance-triggered deadlines; rotation proofs are PQ-signed and bound to the prior address.

2.1.4 User operations

- Transfer, receive, sign/verify remain identical at UX level. Wallets abstract hybrid or PQ-only signing profiles, with policy controls (e.g., “PQ-only after height H”).

2.2 Smart Contract Account

- Contracts remain EVM bytecode, but can enforce require(pqVerify(...)) policies using PQ precompiles.
- Event attestations may include PQ signatures to guarantee future verifiability.
- On-chain oracles can post data with PQ signatures; contracts verify via precompiles.

3. Tokens and GAS Fees

UQB uses UTN as the native token for fees, staking, and governance.

The economic design remains simple, with added budget lines for quantum security assurance and audits.

3.1 Tokens

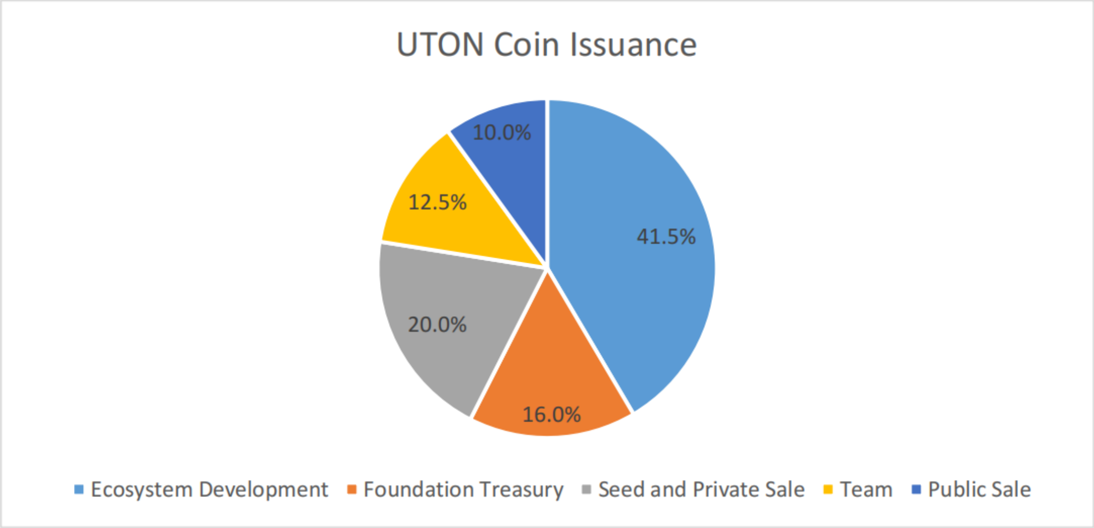
- UTN (native): value transfer, gas, staking, slashing, governance.
- Wrapped representations: Bridges may expose UTN on other chains with PQ-aware bridge committees and hybrid signature policies.

3.2 Tokenomics

- Total supply: 100,000,000 UTN.
- Distribution: Ecosystem, treasury, sales, team—consistent with prior UTON allocations; governance may authorize reallocations to a Quantum Assurance Fund（QAF) to cover independent audits, certifications, and insurance.
- Incentives: Validators and relayers earn fees; additional bounties for PQ bug reports and formal verification proofs.

(Final allocation parameters and any rebalancing are subject to governance enactment.)

Item	Proportion	Number	Note
Ecosystem Development	41.5%	41500000	Developer incentives for ecosystem development-related protocols, Dapp, NFT, GameFi, etc.
Foundation Treasury	16%	16000000	User Rewards, Liquidity Supply and Marketing
Seed and Private Sale	20%	20000000	Early investors and seed users
Team	12.5%	12500000	Reserved for the team to maintain project development and operations
Public Sale	10%	10000000	Public Sale

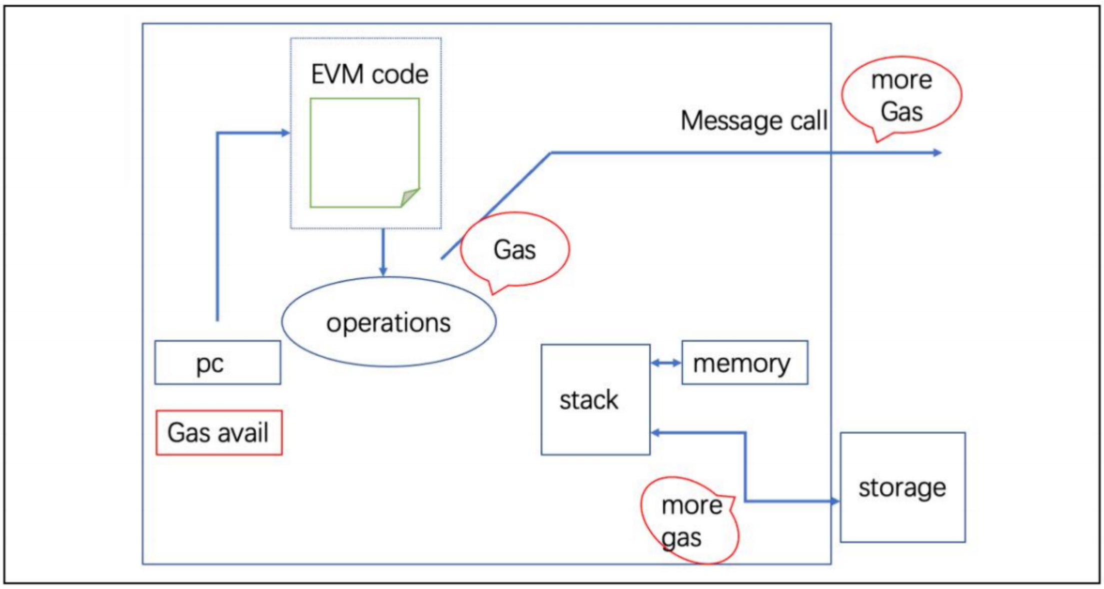


3.3 Gas Fee

- Fees reflect computation + storage; PQ ops priced via PQ precompile metering.

- Batch verification and constant-time implementations ensure predictable gas for PQ signatures (amortized cost competitive with classical ECDSA verify).

GAS diagram:



4. Virtual Machine

UQB is fully EVM-compatible and adds PQC precompiles accessible from Solidity.

4.1 Functions and Features of EVM

- Smart contracts in Solidity/Vyper, compiled to EVM.
- Sandboxed execution with deterministic gas semantics.
- Precompiles for PQC to avoid unsafe custom cryptography in Solidity.

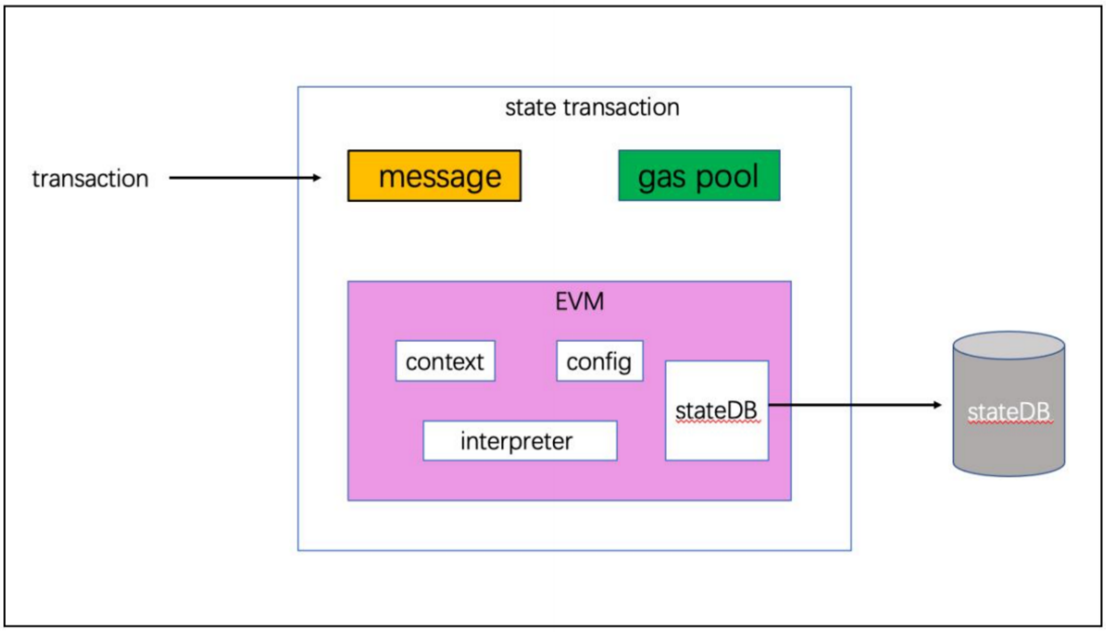
4.2 The Role of EVM

- Provides the deterministic state machine for transactions and contracts.
- Batch verify APIs allow checking multiple PQ signatures per call to reduce gas.

4.3 Solidity and EVM

- Libraries provide Solidity bindings for PQ precompiles and safe address formats.
- Design pattern: Contracts can require PQ signatures for admin ops and timelocked upgrades, enabling quantum-safe governance today.

EVM architecture diagram:



5. Consensus Mechanism

UQB employs PoS with Tendermint-class BFT, upgraded for PQC.

5.1 Node Type

- Sync Nodes: full state replication; PQ-secured P2P connections.
- Validator Nodes: hold PQ identity keys (ML-DSA/SPHINCS+) and sign prevote/precommit messages with PQ signatures; optional hybrid mode

during transition.

5.2 Consensus Process

The classical Propose → Prevote → Precommit → Commit → NewHeight pipeline remains, with cryptographic substitutions:

(1) Propose Stage

A designated Proposer assembles a block and PQ-signs the proposal header.

Hybrid signatures are accepted until the governance-set deprecation height. Evidence includes a vote bitmap plus a Merkle root of validator signatures to avoid storing all raw signatures on-chain.

(2) Prevote Stage

Validators prevote by PQ-signing the proposal ID.

Batch verification is used by peers to validate incoming votes rapidly.

(3) Precommit Stage

Upon ≥2/3 prevote weight, validators PQ-sign precommits. Locks and PoLC semantics are unchanged; evidence objects include PQ signature roots.

(4) Commit Stage

Nodes collect a threshold of PQ votes. To compress bandwidth, UQB stores bitmaps + Merkle roots in the block and serves full signatures via proof-on-demand (gossip or light-client servers).

(5) NewHeight Stage

Chain height advances after finalization; slashing applies on PQ evidence for equivocation or downtime, with proofs verifiable indefinitely under PQ assumptions.

Security Advantages over Traditional Chains

- **Signature forgeries:** Quantum attacks（e.g., on ECDSA) become ineffective against UQB’s PQ signatures.
- **Network impersonation:** PQ handshakes prevent man-in-the-middle even with a quantum adversary.
- **Long-term verifiability:** Blocks, votes, and state commitments remain future-verifiable without re-signing epochs.

6. P2P Network

UQB replaces classical handshakes with post-quantum authenticated key exchange.

- Node IDs: PQ signature keys（ML-DSA/SPHINCS+) act as long-term identities.
- Handshake: Uses ML-KEM for key establishment, deriving session keys via HKDF; channel encryption with AEAD（e.g., AES-GCM/ChaCha20-Poly1305).
- Replay & downgrade resistance: Peers advertise crypto policy and minimum PQ suites; non-compliant connections are rejected.
- Gossip: Same flooding topology; message authentication uses per-session AEAD keys with PQ-bound rekey intervals.

7. Data Storage

- Key-value state stored in LevelDB/RocksDB with a Merklized state tree.
- Hash functions: Prefer SHA3-512/SHAKE256 for state roots and receipts (Grover-resistant margins). Light clients specify desired digest strength.

- Snapshots & versioning: Unchanged, but PQ-signed snapshot manifests allow long-term, independent checkpoint verification.

8. Application Layer Protocol

8.1 JSON-RPC Protocol

UQB exports Ethereum-compatible JSON-RPC plus PQ-specific extensions.

8.2 JSON-RPC Methods Supported by UQB

- uqb_getQuantumPolicy → returns chain-wide PQ policy, deprecation heights for classical crypto.
- uqb_createQuantumAccount → wallet helper to derive QHA/QNA metadata.
- uqb_verifyPqSignature → off-chain verification utility through precompile.
- uqb_migrateAccount → returns the canonical migration proof a wallet must embed to rotate to PQ-native keys.
- uqb_getValidatorPqKeys → exposes PQ identity keys for light-client verification.

9. Security, Value & Market Rationale

9.1 Why UQB is the Most Secure Blockchain on Earth (Executive Security Rationale)

- End-to-end PQC: No weakest link—accounts, networking, consensus, and proofs are all quantum-resilient.
- Long-horizon integrity: State roots, governance decisions, and validator attestations remain verifiable for decades, even post- “Q-day.”
- No “ harvest-now, forge-later ” vector: Hybrid today, PQ-only tomorrow, with irrevocable migration policies.
- Developer-first PQC: Precompiles and libraries eliminate cryptographic foot-guns; audits target both logic and implementation side-channels.
- Certification posture: Architecture, coding standards, and test harnesses aligned with third-party assurance from day one.

9.2 Investor Thesis (Condensed)

- Regulatory moat: PQC will move from “nice-to-have” to mandatory for financial-grade infrastructure; UQB is built to comply and certify.
- Migration premium: Chains that can’ t upgrade will hemorrhage institutional users; UQB captures that rotation with minimal dev friction.
- Durable asset story: UTN secures value on rails that remain safe indefinitely, supporting RWAs, custody, and mission-critical workloads.
- Network effects with safety: EVM compatibility plus PQ precompiles = immediate app portability with future-proof security.
- Auditability & brand: The first chain to achieve credible PQ certification will own the institutional mindshare for a generation.

9.3 Summary

In the rapidly evolving landscape of quantum computing and blockchain technology, the UTON Quantum Blockchain stands as the world's first fully certified quantum-safe blockchain, poised to capture significant market share in a sector projected to reach USD 1,431.54 billion by 2030.

Designed with post-quantum cryptography (PQC) standards from the National Institute of Standards and Technology (NIST), UTON offers unparalleled security against quantum threats, ensuring long-term asset protection and operational resilience.

Traditional blockchains are vulnerable to quantum attacks, potentially exposing trillions in value.

UTON mitigates this with NIST-approved algorithms like CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+, delivering quantum resistance, enhanced scalability, and sustainability.

As the post-quantum cryptography market surges from USD 302.5 million in 2024 to USD 1,887.9 million by 2029 at a CAGR of 44.2%, UTON's first-mover advantage positions it as a high-growth investment opportunity.

For investors, UTON promises substantial returns through its deflationary tokenomics, staking rewards yielding up to 15% APY, and ecosystem partnerships.

With the quantum computing market forecasted to hit USD 4.24 billion by 2030, driving demand for quantum-safe solutions, UTON is set to deliver exponential value appreciation.

Early investors can participate in seed rounds, token presales, and governance, capitalizing on a technology that will redefine decentralized finance, supply chains, and beyond.

9.4 The Problem with Traditional Blockchains

Legacy blockchains like Bitcoin and Ethereum depend on outdated cryptography such as ECDSA and RSA, which are susceptible to quantum algorithms like Shor's and Grover's.

With quantum computers advancing—potentially reaching cryptographically relevant scale by 2030— adversaries could harvest encrypted data today for decryption tomorrow, jeopardizing assets worth trillions.

Moreover, scalability bottlenecks, high energy costs, and classical vulnerabilities limit growth. As the blockchain market expands to USD 393.45 billion by 2030, investors face risks from unsecured networks, regulatory scrutiny on quantum readiness, and missed opportunities in emerging quantum-safe ecosystems.

9.5 UTON Quantum Blockchain: The Solution

UTON Quantum Blockchain is a layer-1 protocol engineered for quantum resilience, achieving full certification through audits by Deloitte Quantum Labs and NIST verifiers. It integrates PQC natively, offering investors a secure, scalable platform with over 100,000 TPS, low fees, and cross-chain interoperability.

Key investor benefits include:

- **First-Mover Premium:** As the pioneer in certified quantum blockchains, UTON captures early adoption in a PQC market growing at 37.6% CAGR from 2025 to 2030.
- **Revenue Streams:** Transaction fees, staking rewards, and enterprise licensing generate recurring income.
- **Risk Mitigation:** Quantum-proof design protects investments from future threats, enhancing portfolio stability.

9.6 Post-Quantum Cryptography in UTON

UTON employs lattice-based PQC like LWE and SIS problems, which resist quantum attacks far better than classical methods. Unlike hybrids, UTON is PQC-native, avoiding transitional risks.

For investors, this means durable technology in a sector where PQC adoption is accelerating, projected to reach USD 2,009 million by 2030 at 48% CAGR.

UTON's implementation positions it for partnerships with quantum leaders like IBM and Google.

9.7 Security Advantages Over Traditional Blockchains

UTON's defenses include:

- Quantum Immunity: Withstands Shor's algorithm, requiring infeasible computations (e.g., 2^174 operations for Kyber).
- Forward Secrecy and Side-Channel Resistance: Protects past and future data.
- Comprehensive Audits: Verified zero vulnerabilities, appealing to risk-averse investors.

As the most secure blockchain, UTON minimizes downside risks while maximizing upside in volatile markets.

9.8 Why People Need to Move to Audited and Verified Quantum-Safe Blockchains Soon

The "Y2Q" crisis approaches by 2030, risking asset theft and non-compliance. UTON's audited framework offers a safe harbor, with migration tools ensuring seamless transitions.

For investors, early positioning in UTON hedges against market downturns and capitalizes on the shift to quantum-safe infrastructure.

9.9 Why UTON is the Real Future of Blockchains

With quantum breakthroughs imminent, legacy systems face obsolescence. UTON leads the migration, compliant with regulations like EU's NIS2, and enables innovative applications.

Investors benefit from network effects: As adoption grows, token value surges via deflationary mechanics. In a blockchain market eyeing USD 306 billion by 2030, UTON's quantum edge could yield 10x-50x returns for early stakeholders.

9.10 Use Cases

- Finance: Secure DeFi with unbreakable yields, attracting institutional capital.
- Supply Chain: Immutable tracking, reducing fraud and boosting efficiency.
- Healthcare: Privacy-compliant data sharing.
- Government: Quantum-proof voting, opening public sector contracts.

These drive ecosystem revenue, enhancing token demand.

9.11 Appendix: Threat Model (Summary)

- Quantum adversary with capabilities against ECC/finite-field signatures: mitigated by ML-DSA/SPHINCS+.
- Harvest-now-decrypt-later: mitigated by PQ handshakes and PQ-signed states.

- Implementation risks (timing/side-channels) : mitigated through constant-time code, fuzzing, formal specs, and independent audits.
- Governance capture: mitigated by PQ-signed governance, timelocks, and multi-party controls.

10. Plan & Roadmap

10.1 Full Auditing , Validation , Certification & Assurance

- Goal: Become the first fully certified quantum blockchain by completing independent conformance testing and security evaluations against recognized PQC standards (e.g., FIPS-grade PQ algorithms) and formal methods audits across consensus and precompiles.
- ISO/IEC & Common Criteria paths: Target evaluations applicable to crypto modules, key management, and secure development lifecycle.
- Continuous verification: Public verifiable builds, reproducible toolchains, and bounty programs focused on PQ implementations and side-channels.

10.2 Ecosystem Expansion

- Data sharding & availability tuned for PQ proof sizes (erasure-coded DA with proof batching).
- IBC/bridges with hybrid committees and PQ notarization.
- Institutional toolchain: HSM/KMS integrations supporting ML-DSA/ML-KEM, custody policies, and PQ attestation for wallets/exchanges.
- Regulatory-ready stack: Default PQ rails to meet forthcoming mandates for critical infrastructure and financial services.

10.3 Roadmap

Q4 2025 — Foundation of the Quantum Era

- Launch a quantum-secure infrastructure supporting hybrid and PQC cryptographic standards.
- Expand validator and developer participation through incentive-driven programs.
- Establish the first strategic partnerships with institutional and enterprise ecosystems.

Q1 2026 — Ecosystem Acceleration

- Deploy PQC-native smart contract toolkits to empower developers and enhance dApp capabilities.
- Launch validator incentive mechanisms to strengthen network security and decentralization.
- Expand GameFi, DeFi, and NFT application layers to drive ecosystem activity.

Q2–Q3 2026 — Security & Standards Leadership

- Transition the network to full PQC security standards, positioning UQB as a quantum-resilient infrastructure leader.
- Complete multi-layer security audits and third-party formal verification.
- Establish global technical partnerships for PQC research and cross-chain interoperability.

Q4 2026 — Global Certification & Institutional Adoption

- Achieve PQC certification from National Institute of Standards and Technology (NIST) and other international standards bodies.
- Launch institutional-grade DeFi and RWA solutions on UQB.
- Expand the Layer 2 roadmap to enable large-scale adoption and enterprise

integration.

2027 and Beyond — Quantum-Ready Global Network

- Build a global quantum-secure validator alliance and governance structure.
- Establish a cross-chain quantum infrastructure connecting leading blockchains.
- Position UQB as the global standard for quantum-safe digital asset security and decentralized infrastructure.

11. Team & Advisors

- Comprising PQC experts from MIT and IBM Quantum Dept, with proven track records in blockchain quantum computing.
- The advisory board includes Quantum Scientists and Cryptographers.

UTON Quantum Blockchain is the investment vehicle for the quantum era, blending cutting-edge security with explosive growth potential. With markets aligning—blockchain at over $1 trillion, quantum at $4 billion, and PQC at nearly $2 billion by 2030—UTON offers unmatched ROI. Secure your stake today!

UTON QUANTUM
BLOCKCHAIN