QUANTUM SHARDED NETWORK (QSN)

Technical Documentation

WHITEPAPER

Next-Generation Post-Quantum Blockchain

with EVM, TVM and QVM support

Version 1.0 | December 2025

https://qsnchain.com

ABSTRACT

Quantum Sharded Network (QSN) is a next-generation blockchain platform designed to address quantum computing threats and meet the scalability requirements of modern decentralized applications. QSN combines three virtual machines (EVM, TVM, QVM), post-quantum cryptography based on NIST standards (Dilithium3, Kyber1024, SPHINCS+), dynamic sharding with theoretical throughput up to 2.6 million TPS, and built-in DeFi primitives at the protocol level.

Key Features:

- Post-Quantum Protection — hybrid Ed25519 + Dilithium3 signatures per NIST standards
- Multi-VM Architecture — support for EVM (Solidity), TVM (FunC) and QVM (Qubit) in one network
- Dynamic Sharding — automatic scaling up to 256 shards per workchain
- Instant Finality — transaction confirmation in ~3 seconds
- Built-in DeFi — AMM, Lending, Flash Loans at protocol level
- Cross-chain Compatibility — bridges with Ethereum, BSC, Polygon, TON, Cosmos

1. INTRODUCTION

1.1 Problems with Existing Blockchains

Current blockchain networks face three key challenges that limit their potential for mass adoption:

Quantum Vulnerability

ECDSA and RSA algorithms used in Bitcoin, Ethereum, and other networks are vulnerable to quantum computer attacks using Shor's algorithm. According to NIST projections, cryptographically relevant quantum computers will appear by 2030-2035. This creates an existential threat to all assets protected by classical cryptography.

Limited Scalability

Ethereum processes about 15 TPS, Bitcoin about 7 TPS. Even Layer 2 solutions don't fully solve the problem as they require periodic synchronization with the main network. Mass adoption requires throughput of hundreds of thousands of transactions per second.

Ecosystem Fragmentation

Division into incompatible networks (Ethereum, TON, Solana, Cosmos) creates barriers for developers and users. The need to learn different programming languages, use different wallets and bridges complicates Web3 interaction.

1.2 QSN Solution

QSN comprehensively solves all three problems by providing a unified platform that:

- Uses post-quantum cryptography (Dilithium3, Kyber1024, SPHINCS+) per NIST 2024 standards
- Provides dynamic sharding with automatic scaling to 100,000+ TPS
- Combines three virtual machines (EVM, TVM, QVM) in a single network
- Offers built-in DeFi primitives and cross-chain bridges

2. ARCHITECTURE

2.1 Multi-Layer Structure

QSN uses a three-layer architecture: Masterchain coordinates the network, Workchains process transactions for different virtual machines, and Shards provide horizontal scaling within each workchain.

Core Network Parameters:

Parameter	Value	Description
Block Time	3 seconds	Block creation time
Block Gas Limit	30,000,000	Gas limit per block
Max TX per Block	1,000	Maximum transactions per block
Min Gas Price	1 Gwei	Minimum gas price
Epoch Length	100 blocks	Epoch duration
Min Validators	4	Minimum validators for consensus

2.2 Masterchain

Masterchain is the coordination layer responsible for global consensus and management:

- Consensus — global BFT + PoS consensus management
- Validator Registry — registration, staking, slashing
- Shard Coordination — load distribution, cross-shard transactions
- Network Parameters — protocol upgrades, governance

2.3 Workchains

Workchain	VM	Language	Purpose
0	QVM	Qubit	Native contracts, DeFi, PQ operations
1	EVM	Solidity	Ethereum compatibility
2	TVM	FunC	TON compatibility

2.4 Dynamic Sharding

Shards automatically split and merge based on load:

- Split — when load > 80%, shard splits into two
- Merge — when load < 20%, two shards merge
- Max shards — up to 256 shards per workchain

Theoretical Maximum TPS Formula:

```
TPS_max = shards × validators_per_shard × block_time⁻¹ × tx_per_block TPS_max = 256 × 21 × 0.33 × 1000 ≈ 2,688,000 TPS
```

3. BFT + PoS CONSENSUS

3.1 Byzantine Fault Tolerant + Proof of Stake

QSN uses a hybrid consensus combining Byzantine Fault Tolerance (BFT) with Proof of Stake (PoS) to achieve high security and energy efficiency.

Key Properties:

- Single-block finality (~3 seconds)
- Tolerates 1/3 Byzantine nodes
- Energy-efficient PoS (unlike PoW)
- Deterministic leader selection

3.2 Consensus Phases

Phase	Timeout	Description
PROPOSE	3000 ms	Leader proposes block
PREVOTE	2000 ms	Validators vote for block
PRECOMMIT	2000 ms	Validators confirm choice
COMMIT	-	Block finalized

Leader (proposer) is selected via round-robin algorithm weighted by active stake. Block finalization requires >2/3 of total validator voting power.

3.3 Staking Parameters

Parameter	Testnet	Devnet	Mainnet
Minimum stake	100 tQSN	100 dQSN	0.1 QSN
Unbonding period	7 days	7 days	7 days
Maximum validators	1,000	1,000	1,000
Activation limit per epoch	32	32	32
Epoch length	100 blocks	100 blocks	100 blocks

3.4 Slashing (Penalties)

Violation	Penalty	Description
Double Vote	5% stake	Voting for different blocks at same height
Surround Vote	10% stake	Attempted surrounding vote
Invalid Proposal	Variable	Proposing invalid block

3.5 Rewards

Parameter	Value
Maximum supply	1,000,000,000 QSN
Annual inflation	0.5%
Blocks per year	~6,307,200
Validator share	80%
Treasury	10%
Burn	10%

4. POST-QUANTUM CRYPTOGRAPHY

4.1 Quantum Computer Threat

Quantum computers with sufficient qubits pose a serious threat to modern cryptography:

- Shor's Algorithm — breaks ECDSA/RSA in polynomial time
- Grover's Algorithm — accelerates brute-force by √N
- Harvest Now, Decrypt Later — collecting encrypted data now for future decryption

According to NIST and leading research centers, cryptographically relevant quantum computers will appear in 2030-2035. This creates urgent need to transition to quantum-resistant algorithms.

4.2 NIST PQC Algorithms

QSN uses algorithms standardized by NIST in 2024:

Algorithm	Type	Key Size	Signature Size	Level
Dilithium3 (ML-DSA)	Signature	1,952 bytes	3,309 bytes	NIST L3
Kyber1024 (ML-KEM)	KEM	1,568 bytes	1,568 bytes	NIST L5
SPHINCS+	Signature	64 bytes	49,856 bytes	NIST L3
Ed25519	Signature	32 bytes	64 bytes	Classic

4.3 Hybrid Mode

For maximum security during quantum transition, QSN uses hybrid signatures:

```
Hybrid Signature = Ed25519(message) || Dilithium3(message)
```

Both signatures must be valid for transaction verification. This provides protection from both classical attacks (Ed25519) and quantum attacks (Dilithium3).

4.4 PQ Signature Thresholds

Operation	Threshold	PQ Required?
Native transfer	< 1000 QSN	No
Native transfer	>= 1000 QSN	Yes
Token deploy	Always	Yes
Token transfer	< 1000 tokens	No
Token transfer	>= 1000 tokens	Yes
NFT deploy	Always	Yes

5. VIRTUAL MACHINES

5.1 QVM (Quantum Virtual Machine)

QVM is QSN's native virtual machine optimized for post-quantum cryptographic operations, DeFi primitives, and high-performance computing.

QVM Features:

- Register-based architecture (256 registers)
- 109 opcodes (87 EVM-compatible + 22 QVM-specific)
- Built-in DeFi opcodes (swap, addLiquidity, borrow)
- Precompiles for PQ cryptography
- Native Qubit language with safe arithmetic

Qubit Contract Example:

```
contract Token { storage { balances: map<address, u256>, totalSupply: u256 } pub fn
transfer(to: address, amount: u256) -> bool { require(self.balances[msg.sender] >= amount)
self.balances[msg.sender] -= amount self.balances[to] += amount return true } }
```

5.2 EVM (Ethereum Virtual Machine)

QSN provides full Ethereum compatibility:

- Solidity contracts without modifications
- Web3.js / ethers.js compatibility
- MetaMask support
- Account Abstraction (ERC-4337)
- Precompiles for Dilithium3, Kyber1024

5.3 TVM (TON Virtual Machine)

TON ecosystem compatibility for porting existing applications:

- FunC contracts
- Asynchronous message model
- Actor model
- BOC (Bag of Cells) serialization

5.4 Precompiled Contracts

Адрес	Контракт	Gas
0x01-0x09	EVM стандартные	Variable
0x0C	Dilithium3Verify	10,000
0x0D	Kyber1024	15,000
0x0E	SPHINCS+Verify	50,000
0x0F	Ed25519Verify	3,000
0x11	HybridVerify	13,000
0x15	Blake3	100 + 10/word
0x100	DeFi AMM	50,000

6. DeFi ECOSYSTEM

6.1 Built-in AMM

QSN includes a native Automated Market Maker at the protocol level, providing high efficiency and low fees compared to contract-based AMMs.

Pricing Formula:

```
x * y = k (constant product formula)
```

- Base fee: 0.3% (30 basis points)
- Multiple pool support
- Automatic routing through multiple pools
- Front-running protection (MEV protection)

6.2 Lending Protocol

Parameter	Value
Collateral factor	75%
Liquidation threshold	80%
Liquidation bonus	5%
Supported assets	QSN, wETH, wBTC, stablecoins

6.3 Account Abstraction (ERC-4337)

- Social wallet recovery
- Multi-signature (multisig)
- Gas sponsorship (Paymaster)
- Transaction batching
- Custom verification logic

7. CROSS-CHAIN BRIDGES

7.1 Supported Networks

Blockchain	Chain ID	Wrapped Token	Light Client	Signatures
Bitcoin	3	wBTC	SPV (PoW)	FROST 51/100
Ethereum	2	wETH	PoS + Beacon	BLS12-381
BSC	56	wBNB	PoSA	secp256k1 14/21
Polygon	137	wMATIC	Heimdall BFT	secp256k1 2/3
TON	300	wTON	Catchain BFT	Ed25519

7.2 Quantum Protection on Bridging

When tokens are bridged they receive full post-quantum protection:

Source	Cryptography	On QSN	Protection
Bitcoin	secp256k1 (ECDSA)	Dilithium3	NIST PQC Level 3
Ethereum	secp256k1 + BLS	Dilithium3	NIST PQC Level 3
BSC	secp256k1 (ECDSA)	Dilithium3	NIST PQC Level 3
Polygon	secp256k1 (ECDSA)	Dilithium3	NIST PQC Level 3
TON	Ed25519	Ed25519 + Dilithium3	Hybrid

7.3 Lock-and-Mint / Burn-and-Release Mechanism

1. Lock - user locks tokens in vault/contract on source chain
2. Relayer - monitors transaction and waits for confirmations
3. Light Client - verifies block via cryptographic proofs
4. Mint - wrapped tokens minted with Dilithium3 quantum protection
5. Burn - on withdrawal tokens are burned, threshold signers sign
6. Release - original tokens released on target chain

7.4 Confirmations and Fees

Blockchain	Confirmations	Time	Fee
Bitcoin	6	~60 min	0.3%
Ethereum	12	~3 min	0.3%
BSC	64	~3 min	0.3%
Polygon	256	~20 min	0.3%
TON	32	~2 min	0.3%

7.5 Bridge Security

- Threshold signatures (FROST 51/100 for Bitcoin, 2/3 for others)
- Light Client verification of blocks for each chain
- Rate limiting: 10 operations/hour per address
- Post-quantum signatures for all wrapped tokens
- Protection from replay, double spending, front-running attacks

8. TOKENOMICS

8.1 QSN Token

Parameter	Value
Ticker	QSN
Maximum supply	1,000,000,000 QSN
Initial supply	100,000,000 QSN
Decimals	18
Inflation	2% annually (decreasing)
Type	Utility + Governance

8.2 Distribution

Category	%	Amount	Vesting
Ecosystem & Grants	30%	300M	4 years linear
Team & Advisors	15%	150M	1 year cliff + 3 years
Private Sale	15%	150M	6 month cliff + 18 months
Public Sale	10%	100M	No restrictions
Treasury	20%	200M	DAO governance
Liquidity	10%	100M	No restrictions

8.3 Token Utility

- Gas — transaction and smart contract execution fees
- Staking — network validation and rewards
- Governance — protocol change voting
- Fees — fee discounts for holders
- DeFi — collateral in lending and liquidity protocols

9. SECURITY

9.1 Threat Model

Threat	Mitigation
51% attack	PoS + slashing + economic barriers
Quantum attack	Dilithium3/SPHINCS+ signatures
Long-range attack	Weak subjectivity checkpoints
Replay attack	Nonce + chain_id in signature
Front-running	MEV protection, private mempool
Eclipse attack	Diversified peers

9.2 Audits

Date	Auditor	Scope	Result
2025-11-28	Internal	Consensus, Crypto	96% PASS
2026-Q2	Trail of Bits	Smart Contracts	Planned
2026-Q4	NCC Group	PQC Implementation	Planned

9.3 Bug Bounty

Severity	Награда
Critical	до $100,000
High	до $25,000
Medium	до $5,000
Low	до $1,000

10. RPC API AND INTEGRATION

10.1 Public Endpoints

Network	URL	Chain ID
Mainnet	https://node.qsnchain.com/mainnet/	99990
Testnet (PyUniq)	https://node.qsnchain.com/testnet/	99991
Devnet	https://node.qsnchain.com/devnet/	99992
QVM Mainnet	https://node.qsnchain.com/qvm/mainnet/	1
QVM Testnet	https://node.qsnchain.com/qvm/testnet/	2
WebSocket	wss://node.qsnchain.com/mainnet/ws	-

10.2 P2P Bootstrap Nodes

Network	Multiaddr	IP:Port
Mainnet	/ip4/72.62.49.117/tcp/30300	72.62.49.117:30300
Testnet	/ip4/72.62.49.117/tcp/30303	72.62.49.117:30303
Devnet	/ip4/72.62.49.117/tcp/30304	72.62.49.117:30304

10.3 MetaMask Setup

1. Open MetaMask -> Settings -> Networks -> Add Network
2. Fill in fields:

- Network Name: QSN Testnet
- RPC URL: https://node.qsnchain.com/testnet/
- Chain ID: 99991
- Symbol: tQSN
- Block Explorer: https://qsnscan.io

10.4 Core RPC Methods

Method	Description
eth_chainId	Get network Chain ID
eth_blockNumber	Current block number
qsn_getBalance	Extended balance (with nonce)
qsn_sendTransaction	Send with PQ signatures
qsn_deployToken	Deploy QRC-20 token
qsn_createWallet	Create PQ wallet
qsn_faucet	Get test tokens
qsn_getValidators	List active validators

11. ROADMAP

2025 Q4 (Completed)

[+] Mainnet launch
[+] EVM compatibility
[+] Post-quantum signatures (Dilithium3)
[+] Testnet (PyUniq) active
[+] JSON-RPC API (150+ methods)

2026 Q1

- TVM full integration
- Cross-chain bridges (Ethereum, BSC)
- Mobile wallet (iOS, Android)
- Developer SDK

2026 Q2

- QVM v2 with ZK-proofs
- Privacy transactions
- DEX aggregator
- NFT marketplace

2026 Q3-Q4

- Full sharding (256 shards)
- 1M+ TPS
- Enterprise solutions
- Governance DAO

12. CONCLUSION

Quantum Sharded Network represents the next step in blockchain technology evolution. By combining post-quantum cryptography, scalable sharding, and multi-VM architecture, QSN is prepared for quantum-era challenges while maintaining compatibility with existing ecosystems.

Key advantages of QSN:

- Quantum Resistance — protecting assets from future quantum attacks
- Scalability — up to 2.6M TPS theoretical, 100k+ practical
- Universality — support for EVM, TVM and native QVM
- DeFi-ready — built-in AMM, Lending, Flash Loans
- Interoperability — bridges with major blockchains

REFERENCES AND RESOURCES

1. *NIST Post-Quantum Cryptography Standards (2024)*
2. *Dilithium: Digital Signatures from Module Lattices*
3. *Kyber: CCA-secure Module Lattice-based KEM*
4. *BFT Consensus: Practical Byzantine Fault Tolerance*
5. *Ethereum Yellow Paper*
6. *TON Whitepaper*

CONTACTS

- Website: https://qsnchain.com
- Explorer: https://qsnscan.io

Document created: 2025-12-06